CREATING AN IKE IPSEC TUNNEL BETWEEN AN INTERNET SECURITY ROUTER AND A WINDOWS 2000/XP PC

Release date: 11/12/2003

1 Introduction

This application note details the steps for creating an IKE IPSec VPN tunnel between an ASUS Internet Security Router and a PC running Microsoft Windows 2000 or XP. It is assumed that both sides have static IP address for the WAN interface, and a default route configured. All settings and screen dumps contained in this application notes are taken from a Microsoft Windows 2000/XP, and an ASUS Internet Security Router. You may change the IP address, subnet mask and default gateway IP address of any device to match your true network environment.

2 Network Setup

Connect all the devices as indicated in Figure 2.1. The IKE IPSec tunnel ends at the Internet Security Router and PC2. Note that in the actual applications, the Internet Security Router and the Windows 2000/XP PC are most likely connected via the Internet instead of a switch as shown in Figure 2.1.

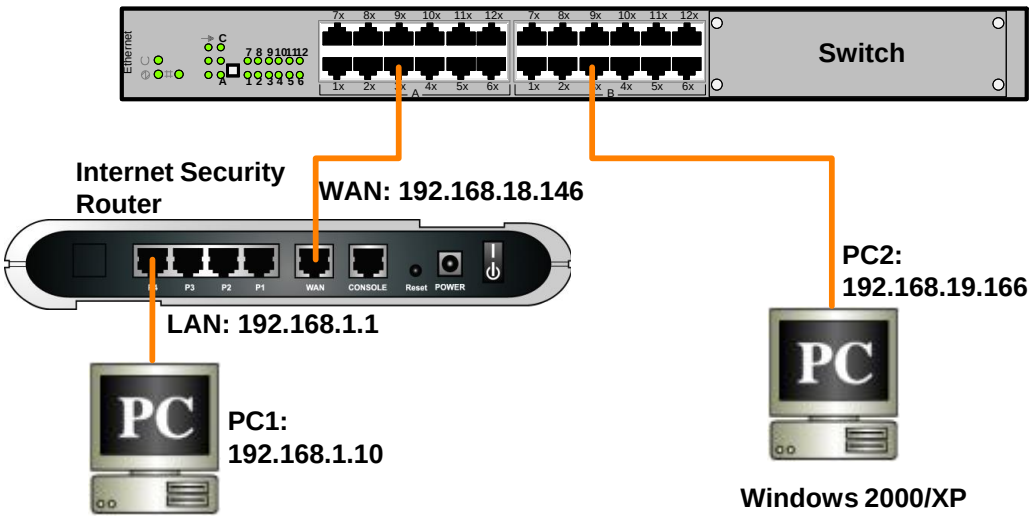


Figure 2.1. Network Diagram

2.1 Configure the IP Address of the Windows PC – PC2

1. Open the “Internet Protocol (TCP/IP) Properties” dialog box
   a) For Windows 2000, click on “Start” **è** select “Settings” **è** click on “Network and Dial-up Connections” icon **è** right click on “Local Area Connection” icon or the icon that represents your PC’s network card **è** select “Properties” **è** double click on “Internet Protocol (TCP/IP)”.
   b) For Windows XP, click on “Start” **è** select “Control Panel” **è** click on “Network Connections” icon **è** right click on “Local Area Connection” icon the icon that represents your PC’s network card **è** select “Properties” **è** double click on “Internet Protocol (TCP/IP)”.
2. Set a static IP address – 192.168.19.166 (see Figure 2.2)
   a) Click on “Use the following IP address:” radio button.
   b) Enter IP address, subnet mask and default gateway as illustrated in Figure 2.2.

Copyright 2003, ASUSTeK Computer, Inc.

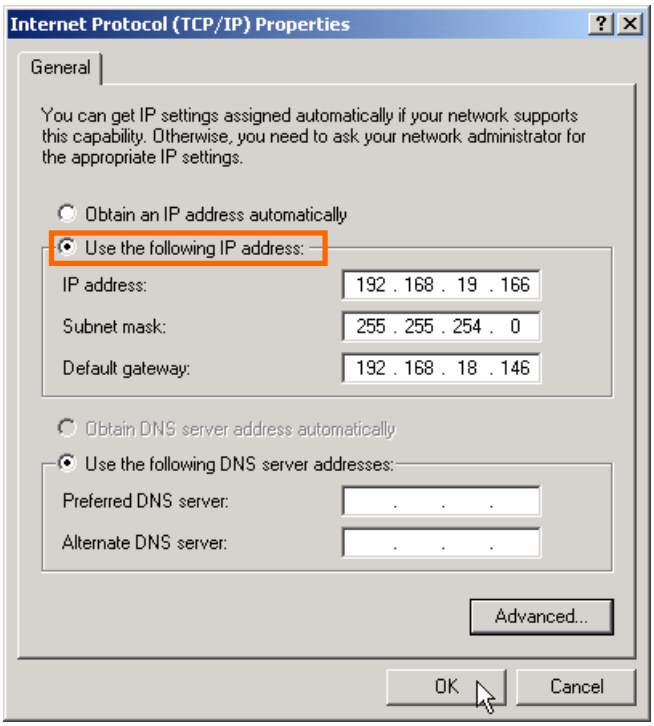


Figure 2.2. Configure the IP address of the Windows 2000/XP PC

2.1.1 Verify the Routing Table in the Windows 2000/XP

After the IP address and default gateway have been properly configured for your PC, enter "route print" command in the Command Prompt window to verify the routing table.

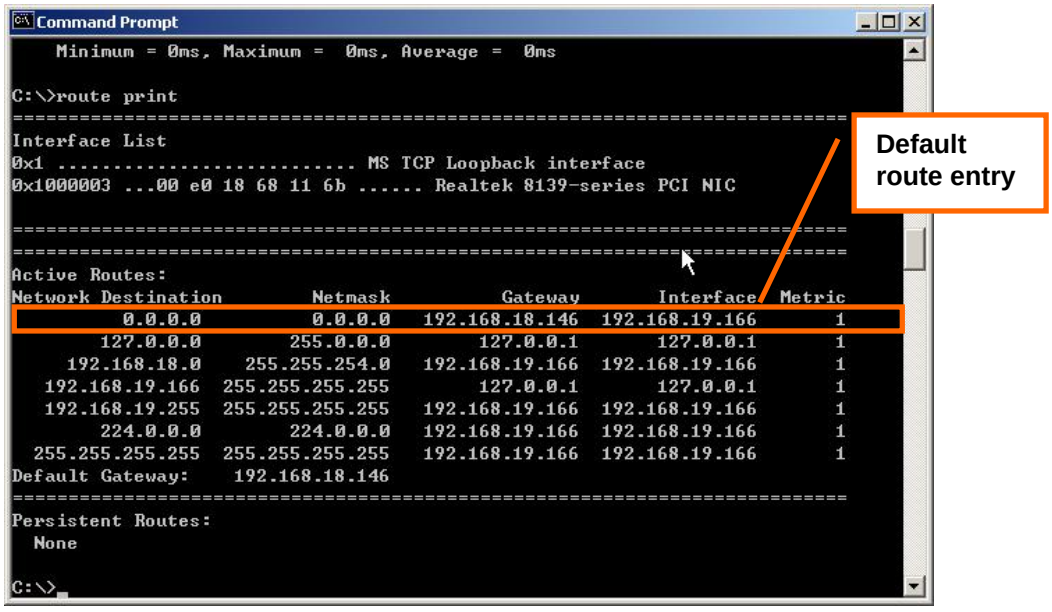


Figure 2.3. Verify the Routing Table in Windows 2000/XP

Make sure that the default gateway is set to 192.168.18.146 in the default route entry. Note that the default route entry is indicated by "0.0.0.0" for both the network destination and netmask.

Copyright 2003, ASUSTeK Computer, Inc.

2.2 Configure the IP Address of the Internet Security Router

You need to login as admin in order to configure the settings for the Internet Security Router.

2.2.1 Configure the WAN Port

Click on the **"WAN"** menu and then click on the **"WAN"** submenu to access WAN Configuration page. Make sure the settings for IP address, subnet mask and the gateway address are set exactly as shown in Figure 2.4. You may ignore the settings for the primary and secondary DNS settings.

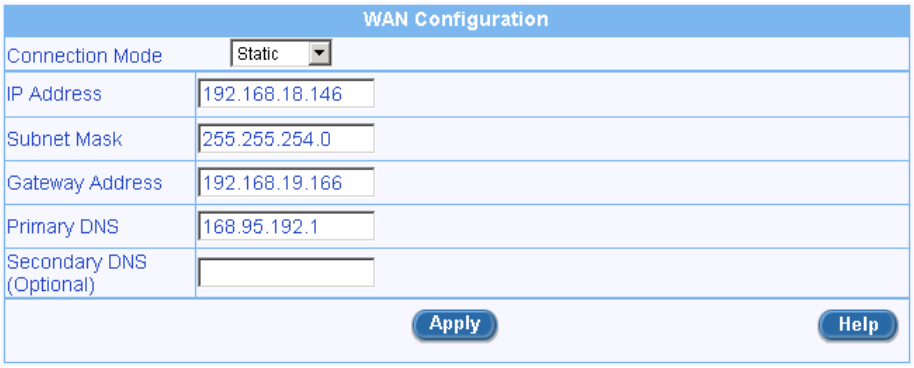


Figure 2.4. Configure WAN Port for the Internet Security Router

2.2.2 Configure the LAN Port

Click on the **"LAN"** menu and then click on the **"IP"** submenu to access LAN Configuration page. Make sure the settings for IP address, and subnet mask are set exactly as shown in Figure 2.5.

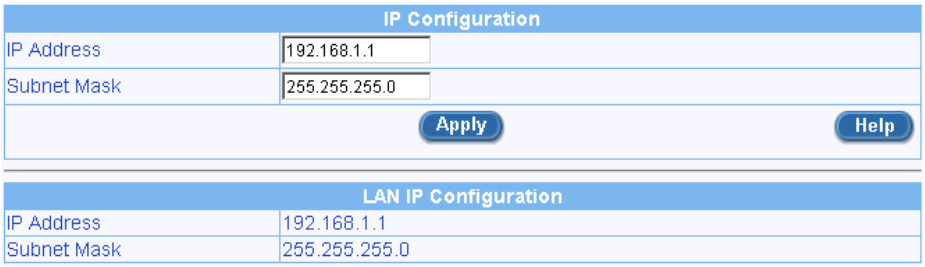


Figure 2.5. Configure LAN Port for the Internet Security Router

2.2.3 Verify the Routing Table in the Internet Security Router

Click on the **"Routing"** menu to access Routing Configuration page. Make sure that a default route is exactly the same as what is shown in Figure 2.6. Default route is indicated by "0.0.0.0" for both the destination IP and the destination netmask.

Copyright 2003, ASUSTeK Computer, Inc.

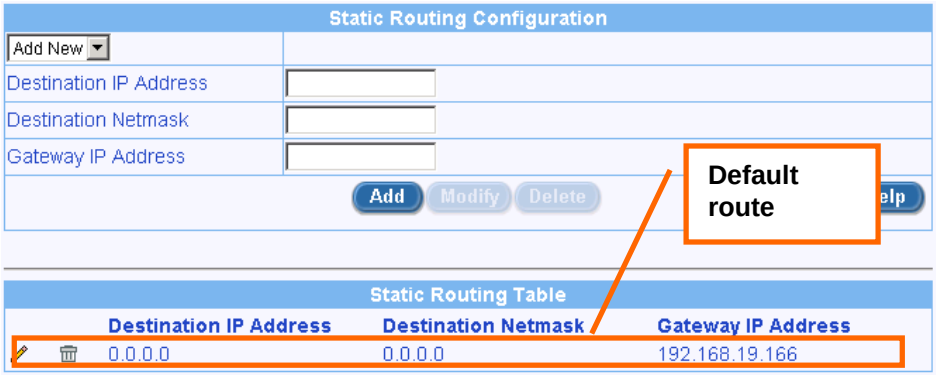


Figure 2.6. Routing Table in the Internet Security Router

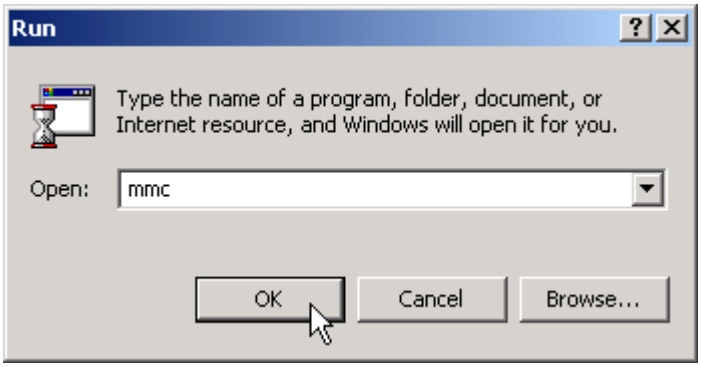
3 Configure IKE IPSec VPN Settings on Windows 2000/XP Using Automatic Keying

Note that Microsoft Windows OS does not support manual key mode for IKE IPSec VPN. Only automatic keying using preshared key will be demonstrated in this document. Three steps are involved this configuration:

- Create a custom MMC (Microsoft Management Console)
- Configure VPN policies in Windows 2000/XP
  - Configure an outbound VPN policy in Windows 2000/XP
  - Configure an inbound VPN policy in Windows 2000/XP

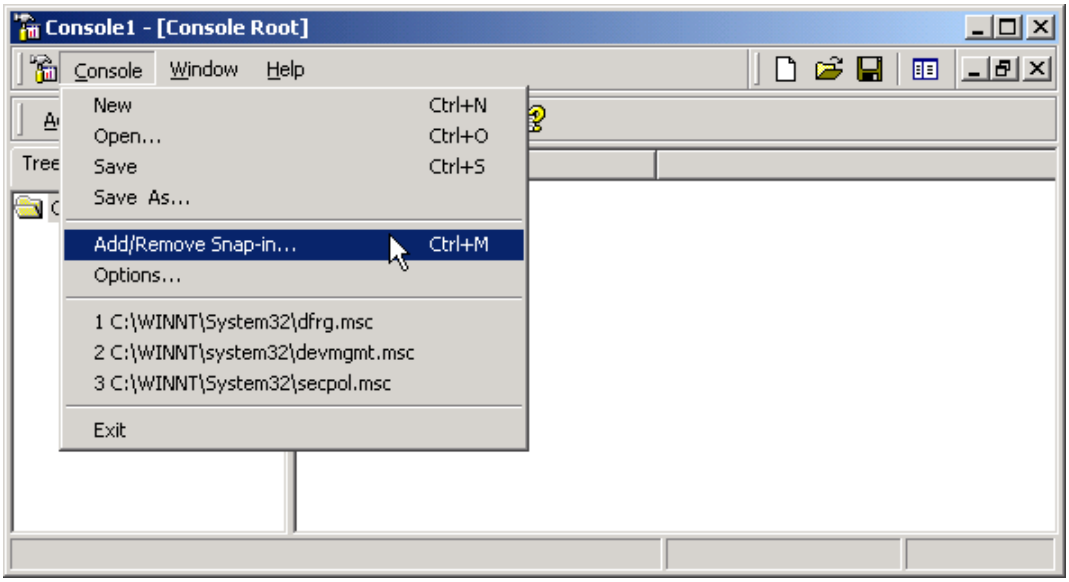
3.1 Create a Custom MMC (Microsoft Management Console) Console

1. Start the MMC console: From the Windows desktop, click on **"Start"**, and then click on **"Run"**. Enter **"mmc"** in the pop-up "Run" dialog window (as shown in the figure below) and then click on the **"OK"** button to continue.

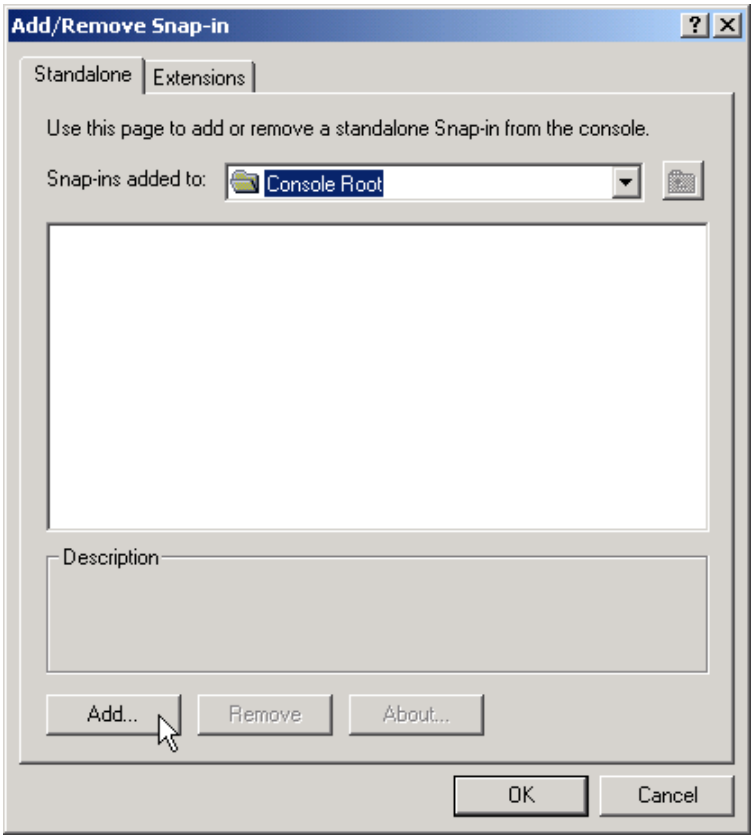


2. The MMC console window displays. Click on the **"Console"** menu, and then select the **"Add/Remove Snap-in…"** submenu.

Copyright 2003, ASUSTeK Computer, Inc.

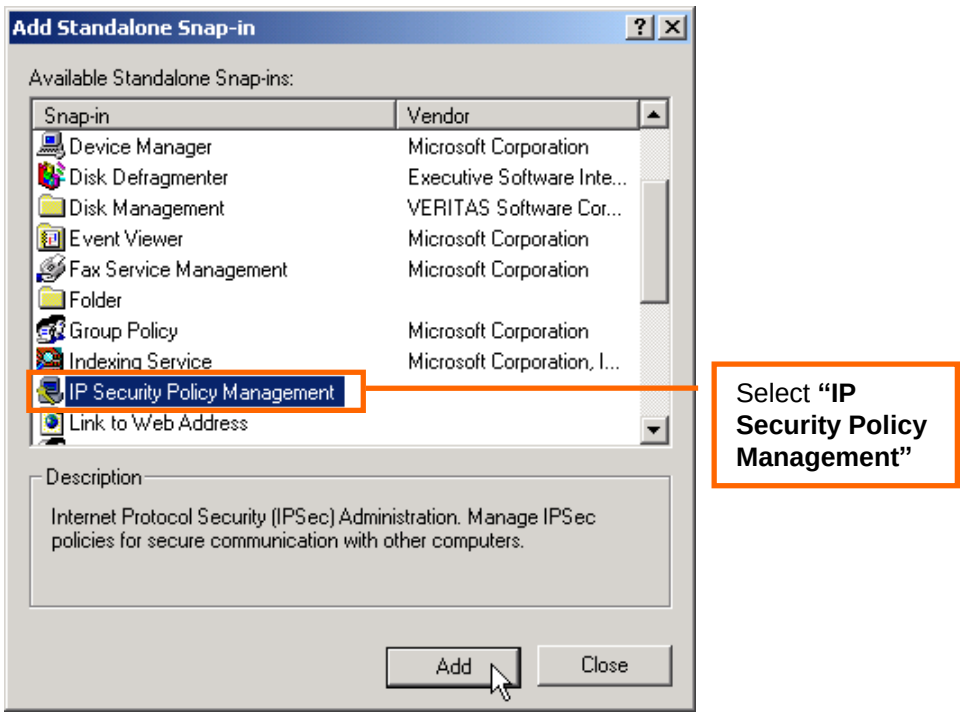


3. In the Add/Remove Snap-in dialog box, click on the **"Add"** button to continue.

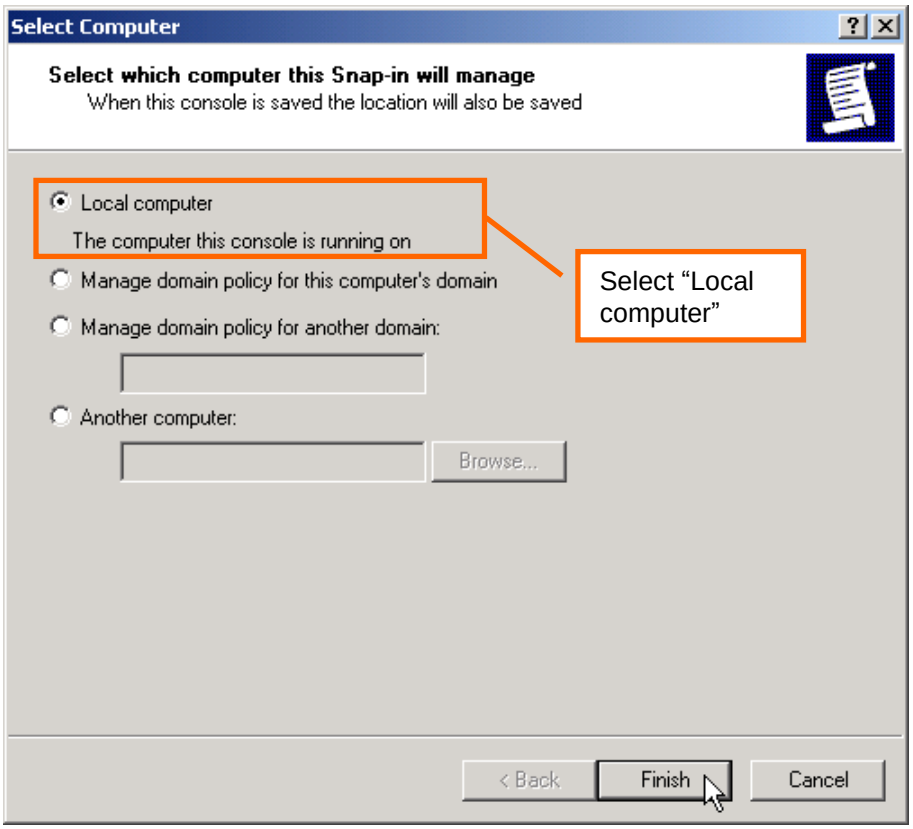


4. In the Add Standalone Snap-in dialog box, select **"IP Security Policy Management"** (you may need to scroll down the list to see this item) and then click on the **"Add"** button to continue.

Copyright 2003, ASUSTeK Computer, Inc.

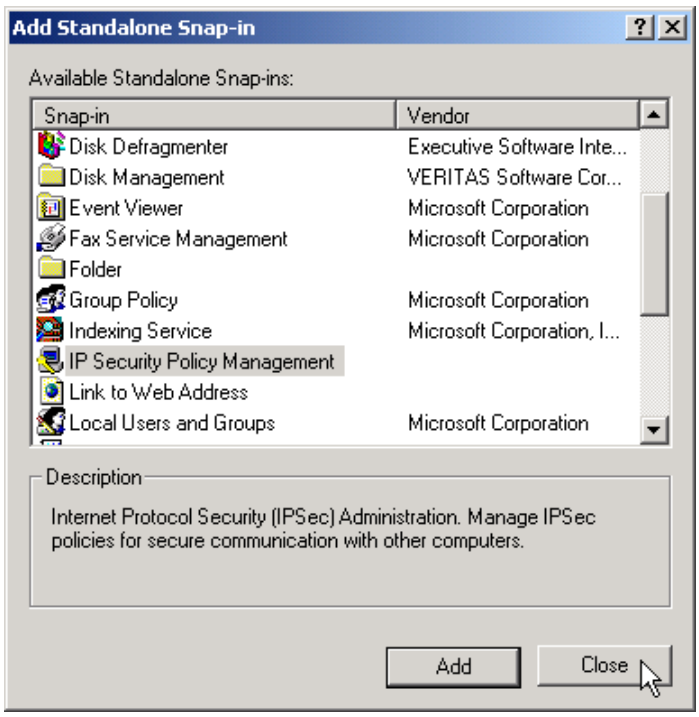


5. Select **"Local computer"** which will be managed by this IP security policy and click the **"Finish"** button.

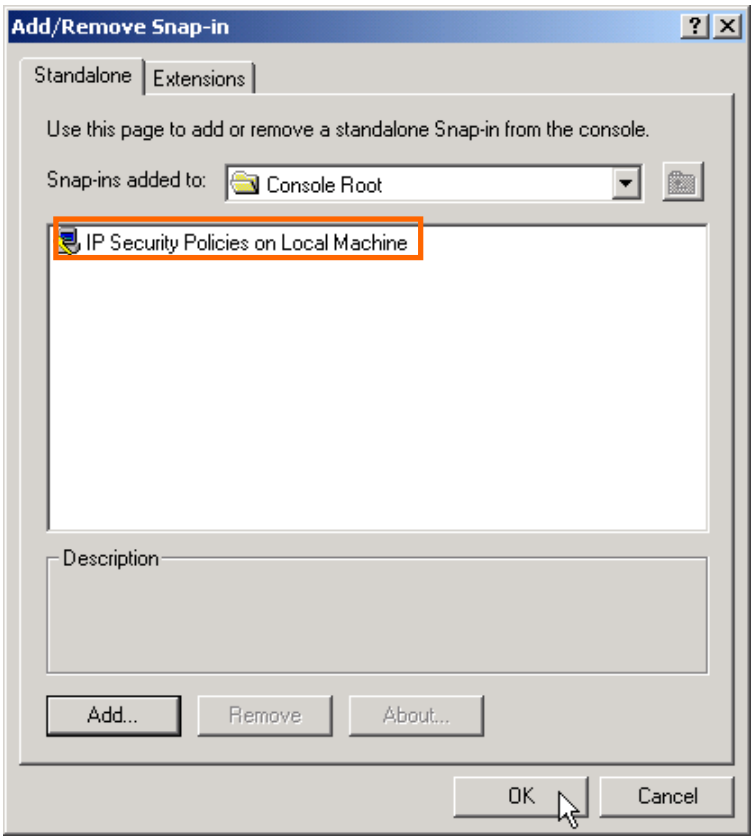


6. Click the **"Close"** button.

Copyright 2003, ASUSTeK Computer, Inc.



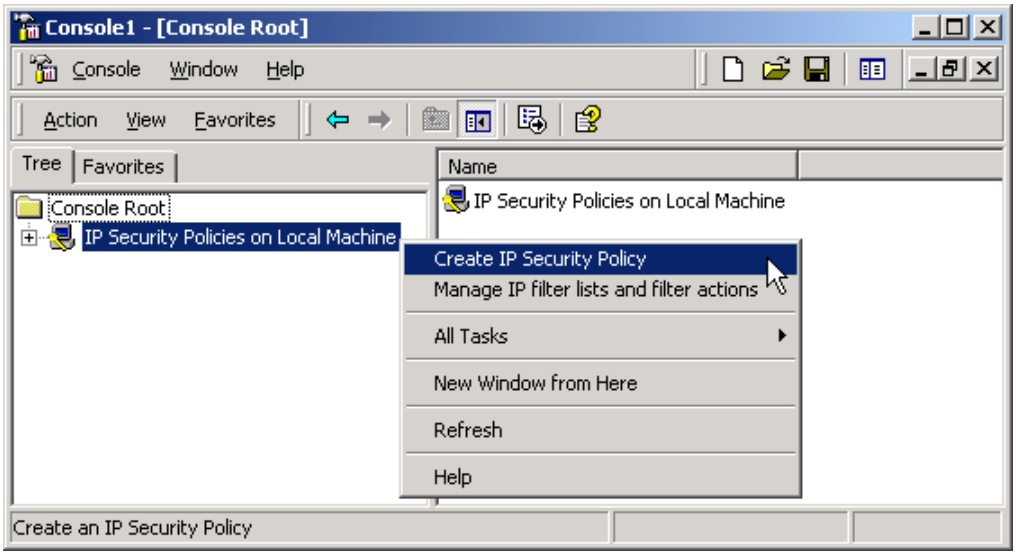
7. You can see that "IP Security Policies on Local Machine" is added. Click the **"OK"** button to return to the MMC console window.



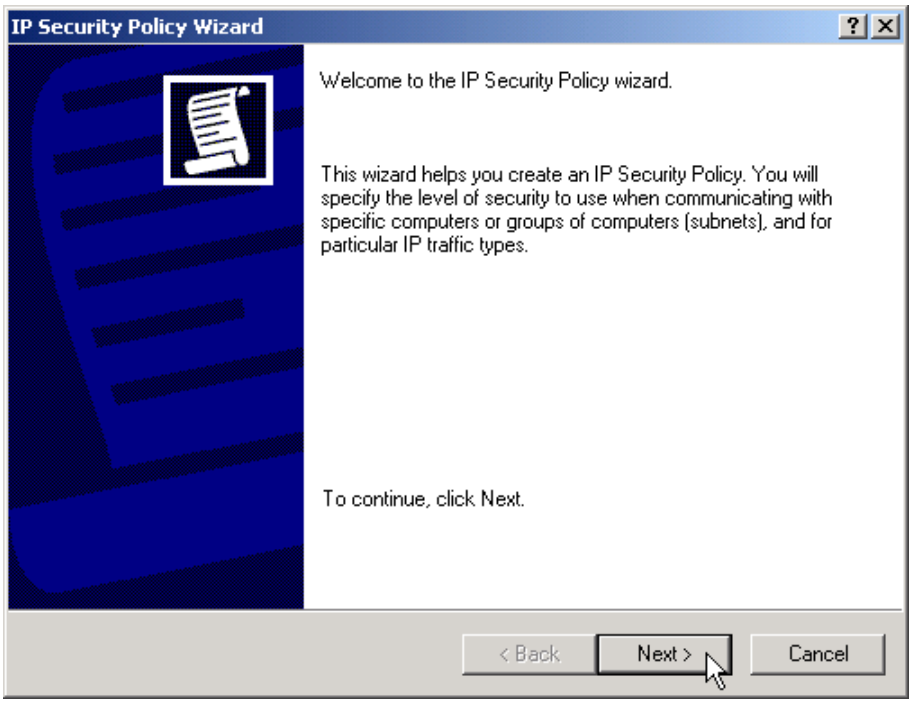
3.2 Configure VPN Policies in Windows 2000/XP

3.2.1 Configure an Outbound VPN Policy in Windows 2000/XP

1. In the MMC console window, right-click on the **"IP Security Policies on Local Machine"** (on the left hand pane of the MMC console window) and then select **"Create IPSec Security Policy"** from the context menu as shown in the following figure.

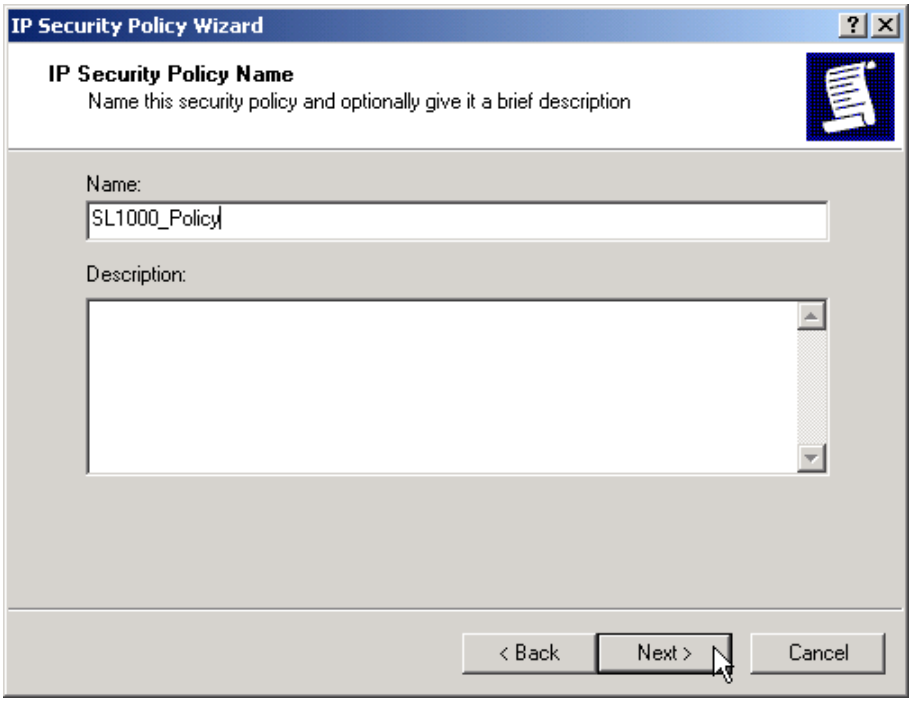


2. "IP Security Policy Wizard" dialog box displays. Click the **"Next"** button to continue.

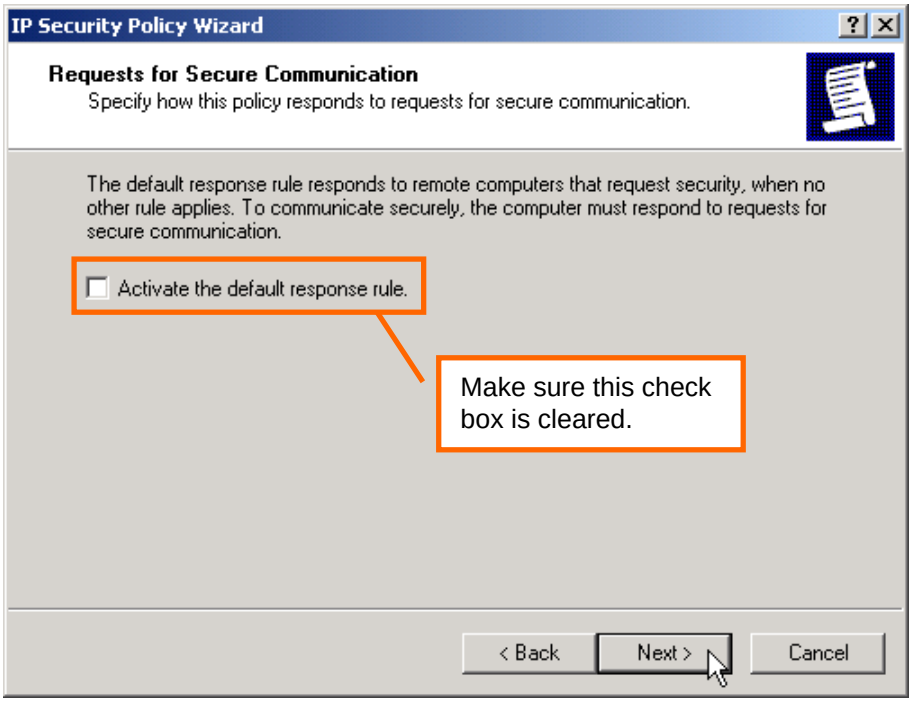


3. Name the IP security policy, **"SL1000_Policy"**, and then click the **"Next"** button to continue. Note that you may enter a detail description for this policy in the **"Description"** text box.

Copyright 2003, ASUSTeK Computer, Inc.

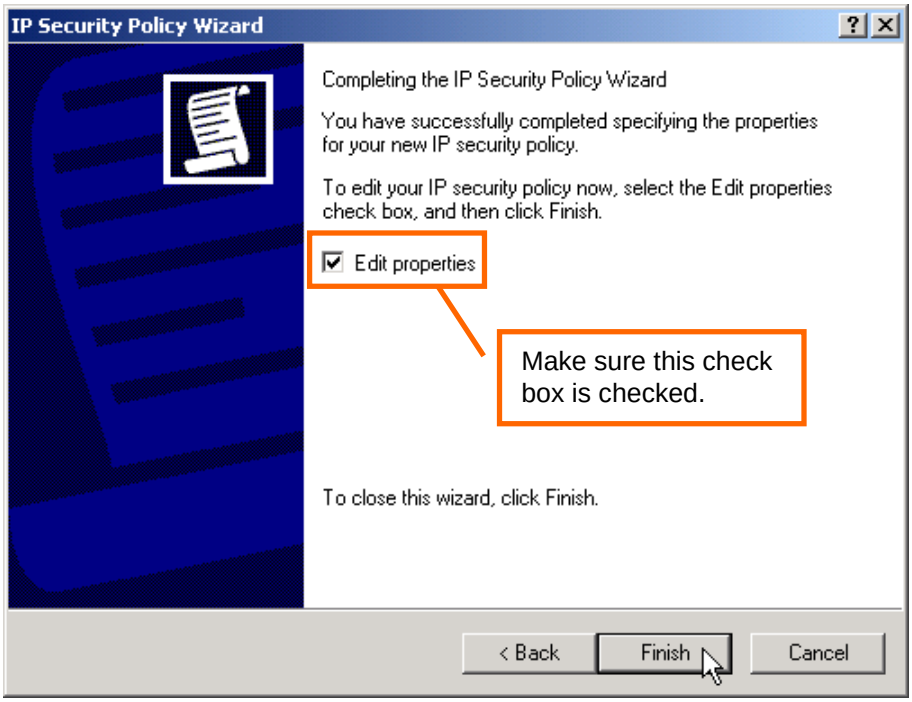


4. Clear the **"Activate the default response rule"** check box, and then click the **"Next"** button to continue.

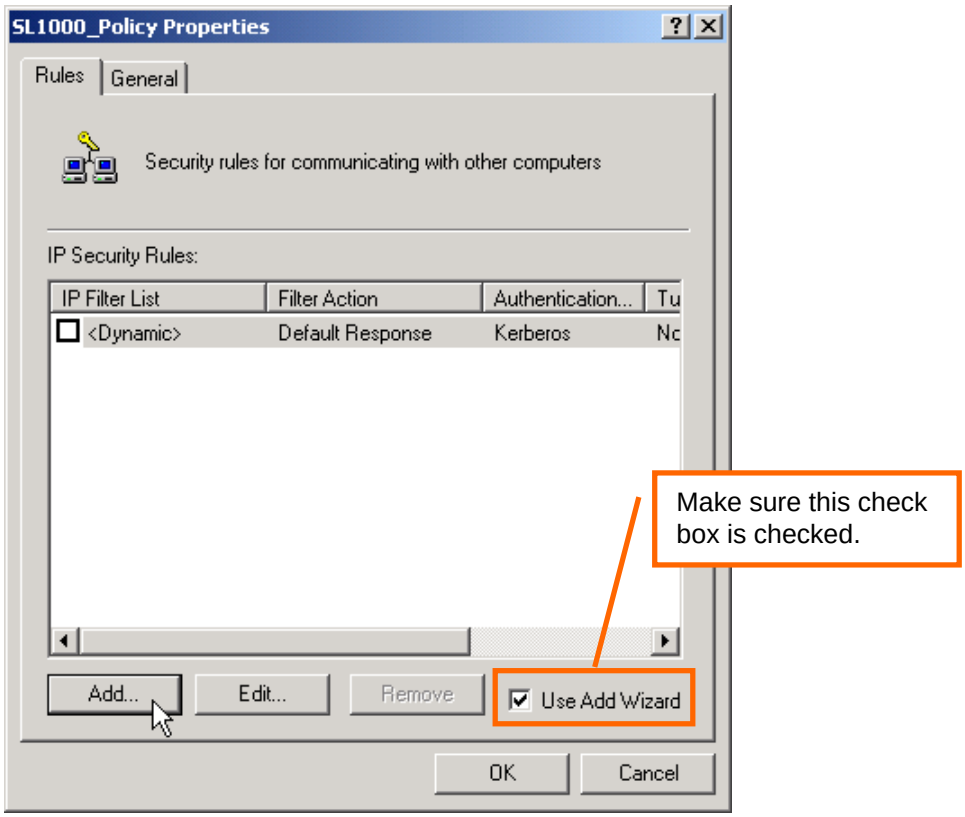


5. Make sure the **"Edit Properties"** check box is checked (it is by default), and then click the **"Finish"** button.

Copyright 2003, ASUSTeK Computer, Inc.

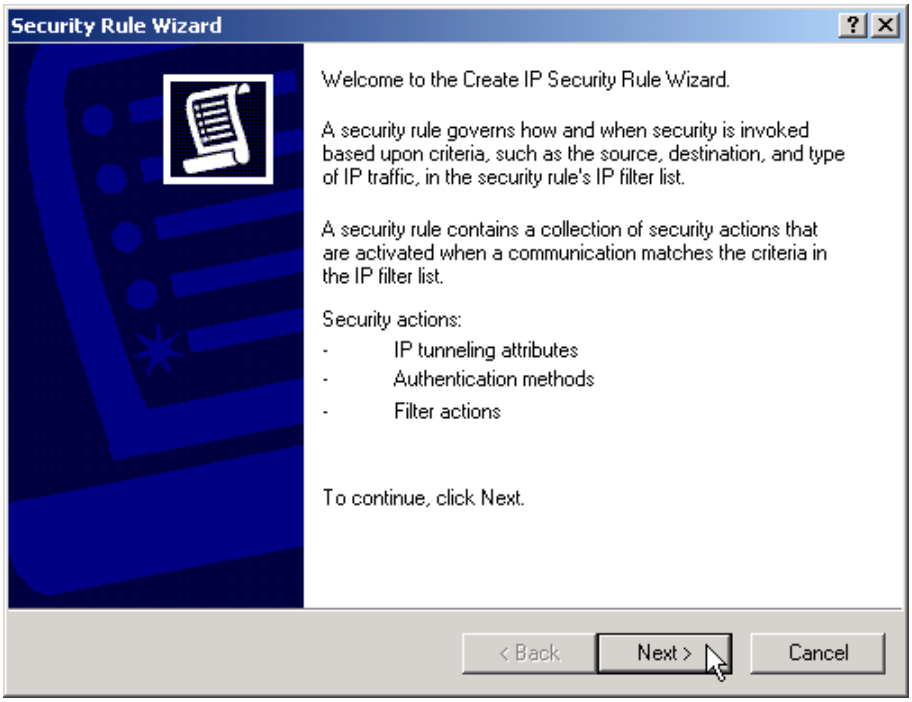


6. In the "SL1000_Policy Properties" dialog box, make sure that the **"Use Add Wizard"** check box in the lower-right corner is checked, and then click the **"Add"** button to start the Security Rule Wizard.

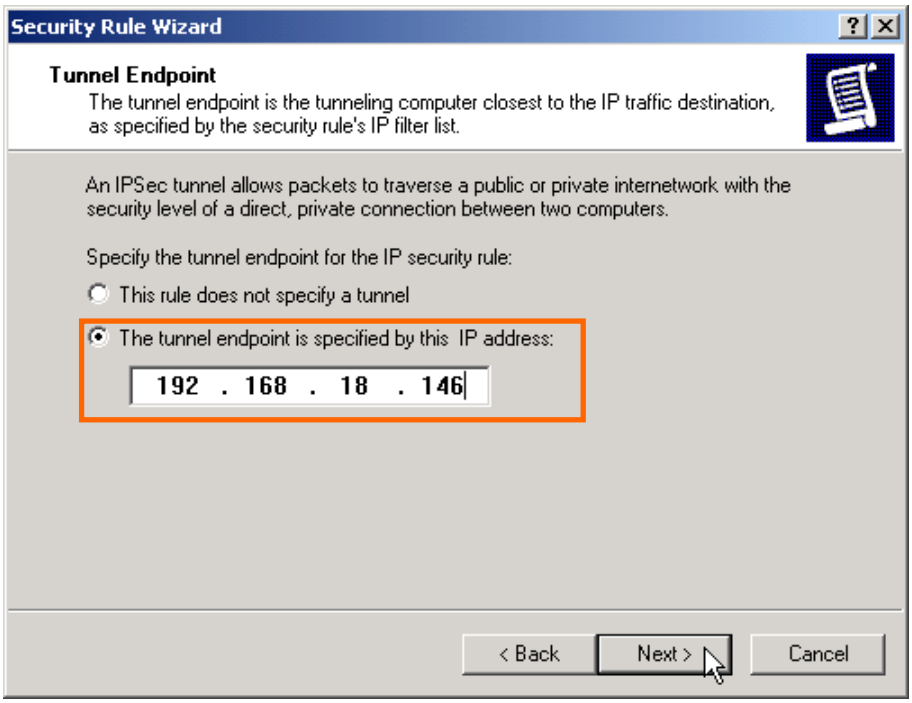


7. Click the **"Next"** button to continue.

Copyright 2003, ASUSTeK Computer, Inc.

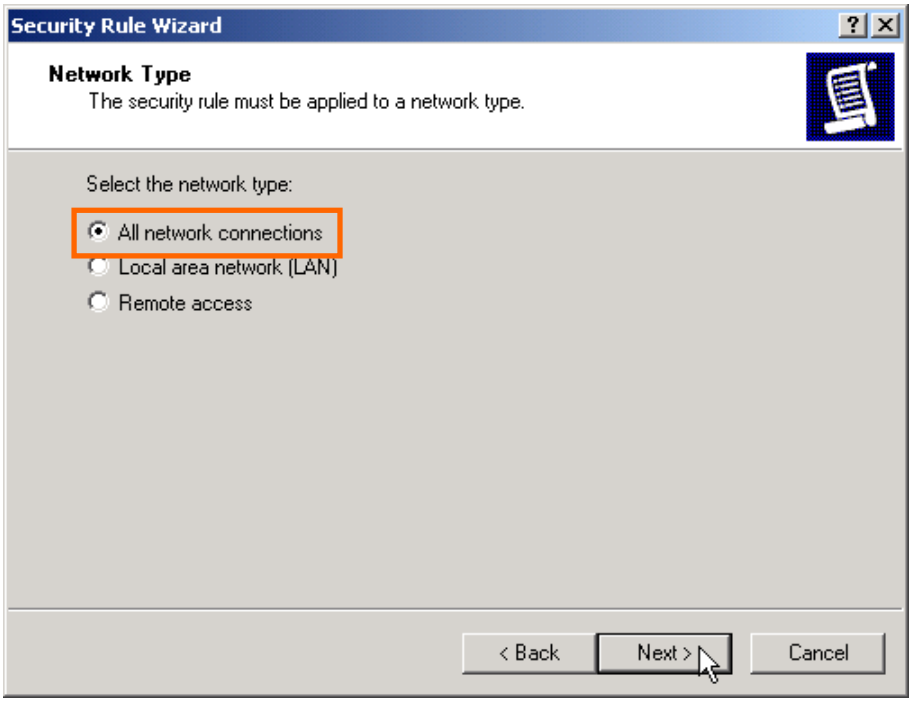


8. Select **"The tunnel endpoint is specified by this IP address:"**, enter **"192.168.18.146"** as the tunnel endpoint for this rule and then click the **"Next"** button to continue.

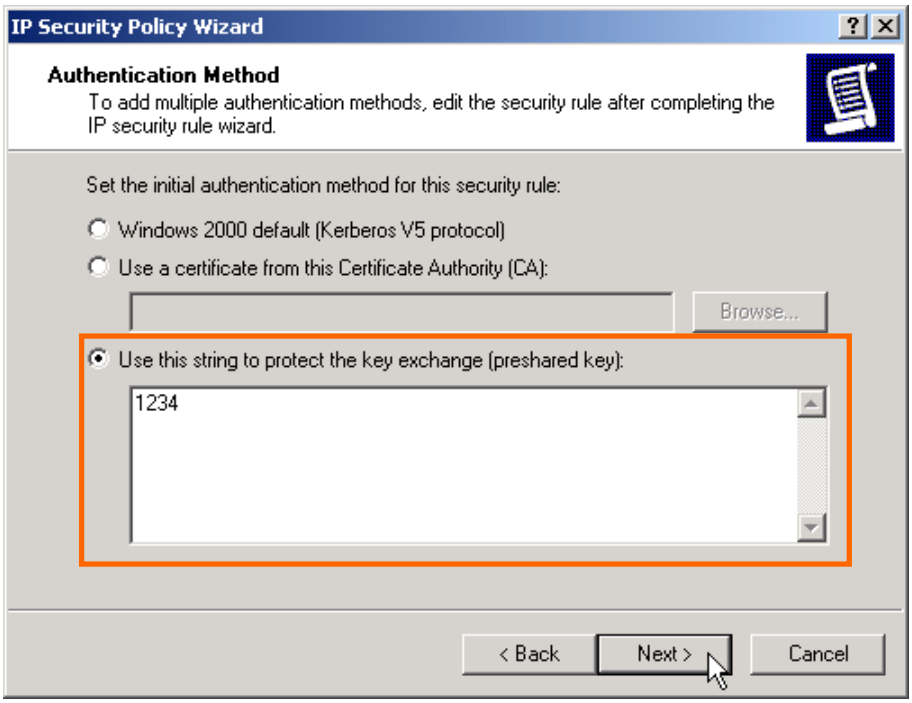


9. Select **"All network connections"** as the network type and then click the **"Next"** button to continue.

Copyright 2003, ASUSTeK Computer, Inc.

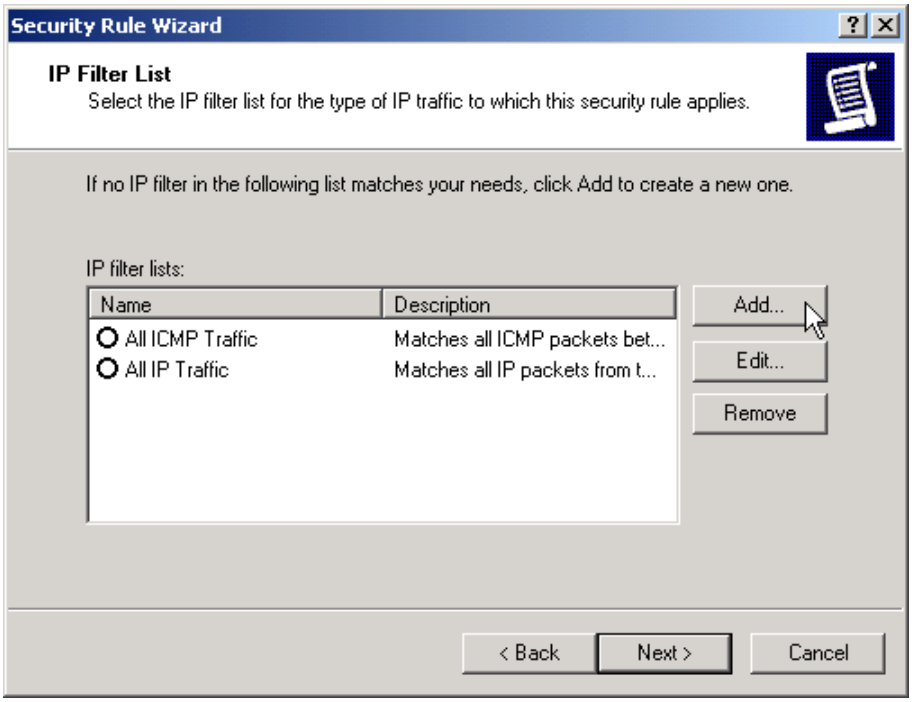


10. Select **"Use this string to protect the key exchange (preshared key):"** as the authentication method and enter **"1234"** as the preshared key. Make sure that this preshared key matches what is configured for the Internet Security Router. To make it more secure, you may choose a longer string. Note that you must not use a blank string for the preshared key. Click the **"Next"** button to continue.

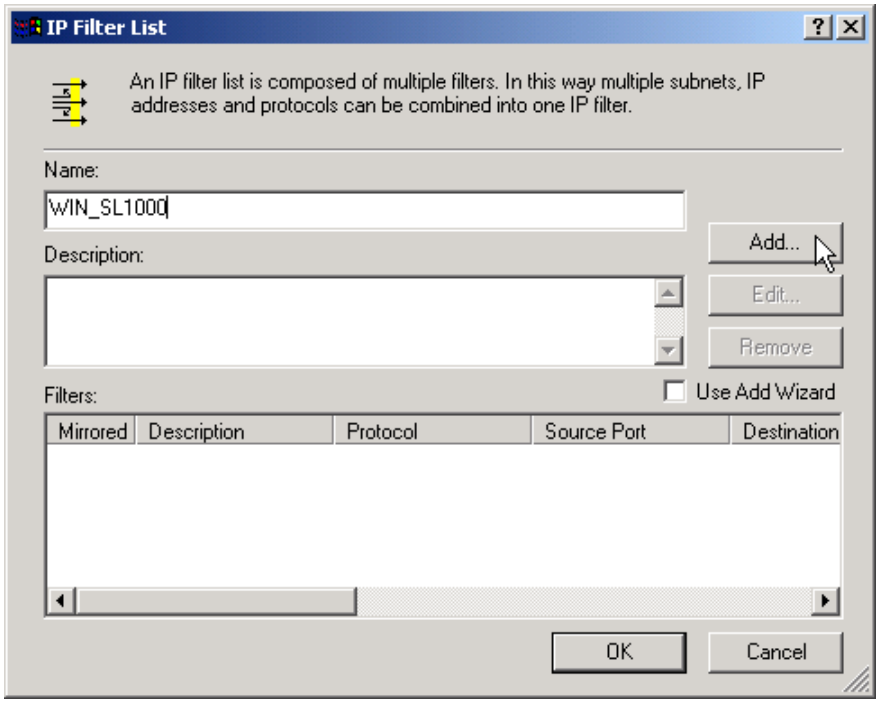


11. In the IP Filter List dialog box, click the **"Add"** button. A list of IP filter is displayed.

Copyright 2003, ASUSTeK Computer, Inc.

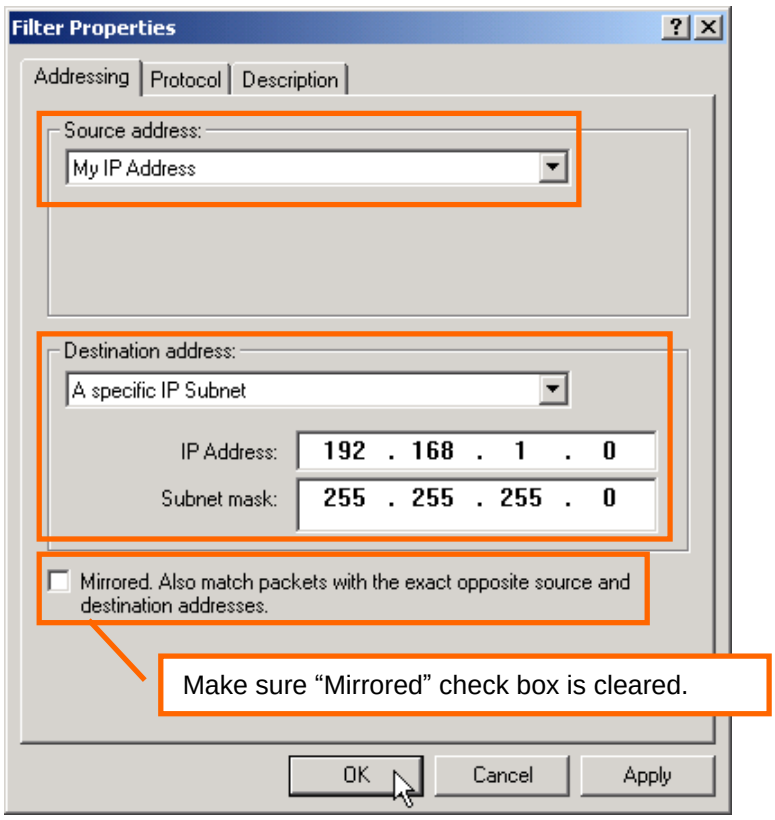


12. Name your filter **"WIN_SL1000"** and click the **"Add"** button to continue.

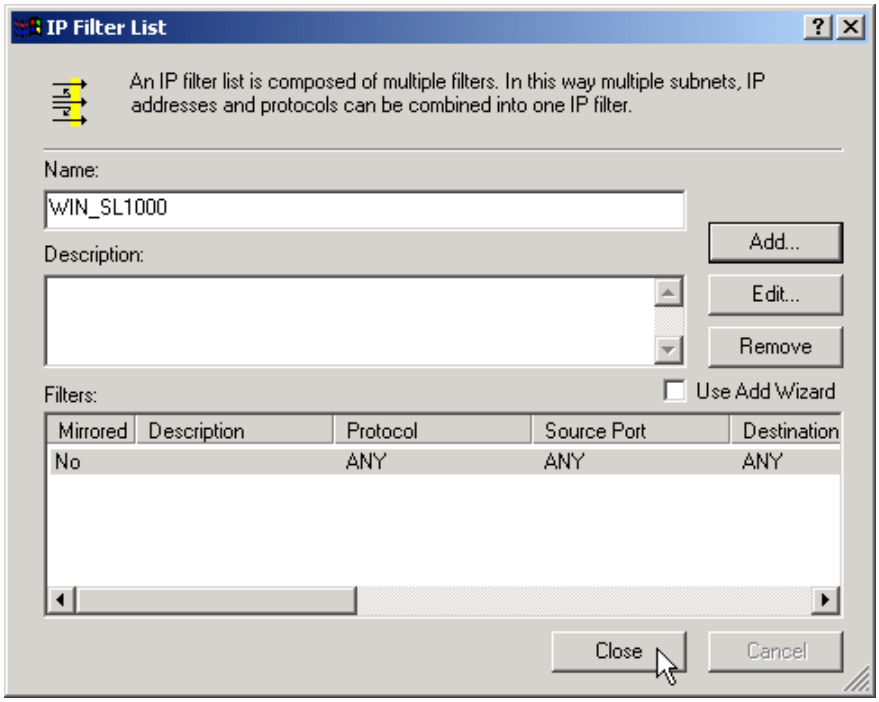


13. Select **"My IP Address"** as the Source address, select **"A specific IP Subnet"** and enter "**192.168.1.0/255.255.255.0"** as the Destination address. Clear the **"Mirrored"** check box and then click the **"OK"** button to continue.

Copyright 2003, ASUSTeK Computer, Inc.

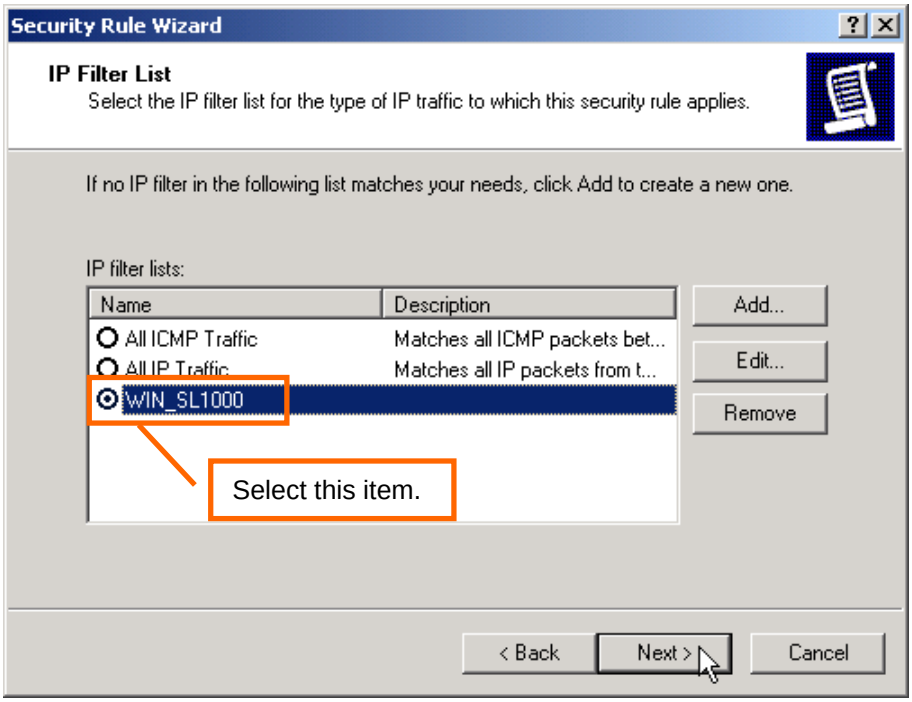


14. Click the **"Close"** button to close the IP Filter List dialog box.

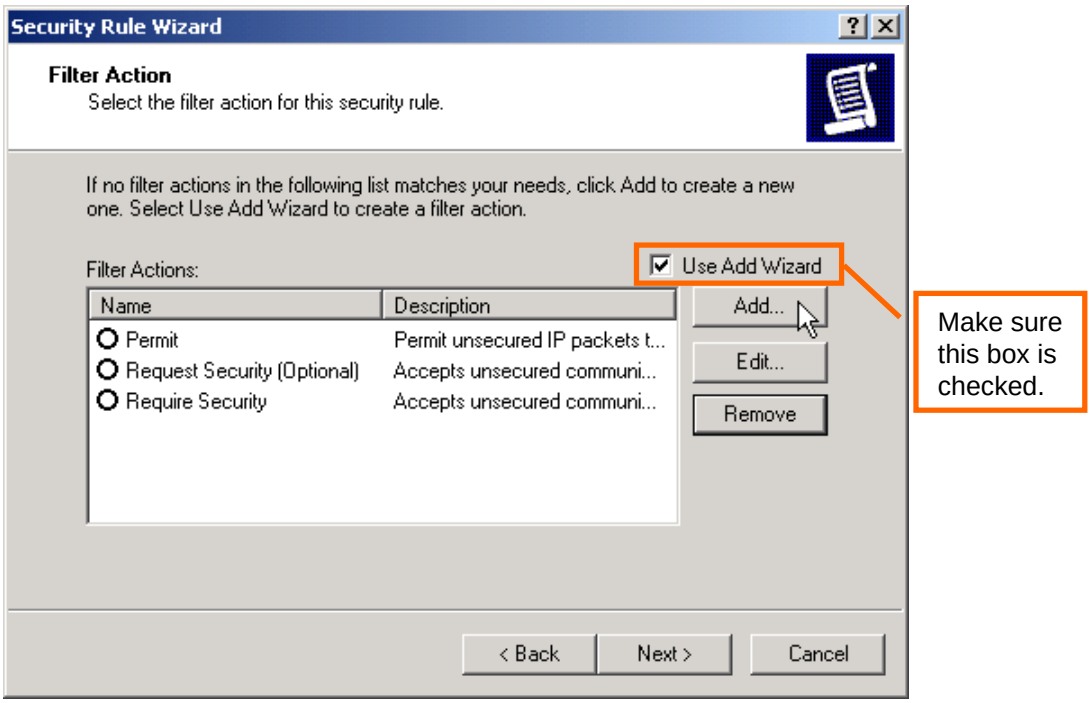


15. In the Security Rule Wizard dialog box, select the newly created IP filter, **"WIN_SL1000"**, and click the **"Next"** button to configure Filter Action.

Copyright 2003, ASUSTeK Computer, Inc.

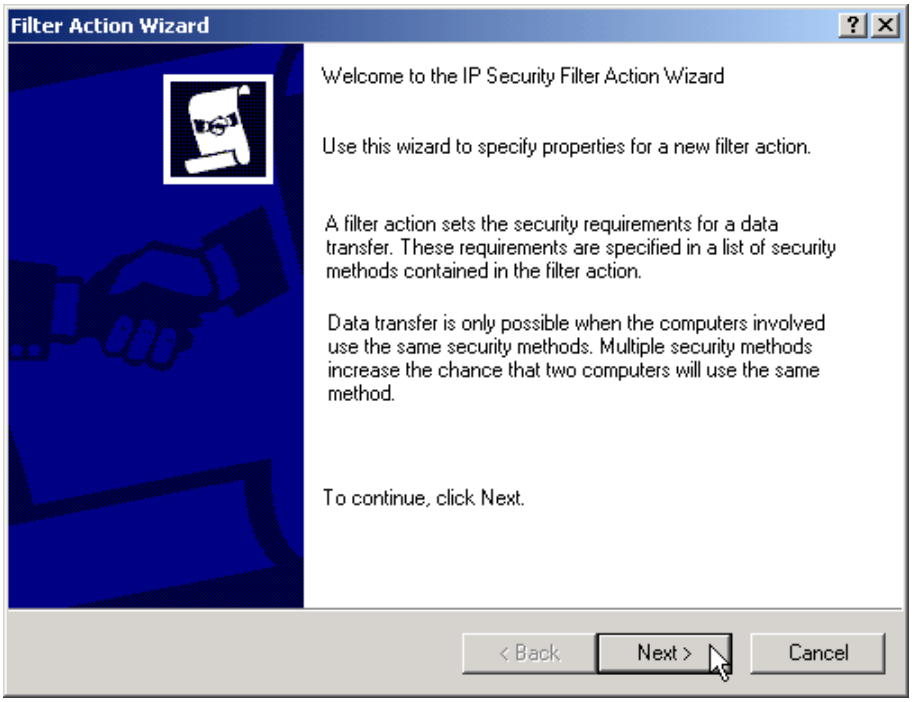


16. In the Filter Action dialog box, check the **"Use Add Wizard"** check box and then click the **"Add"** button to continue.

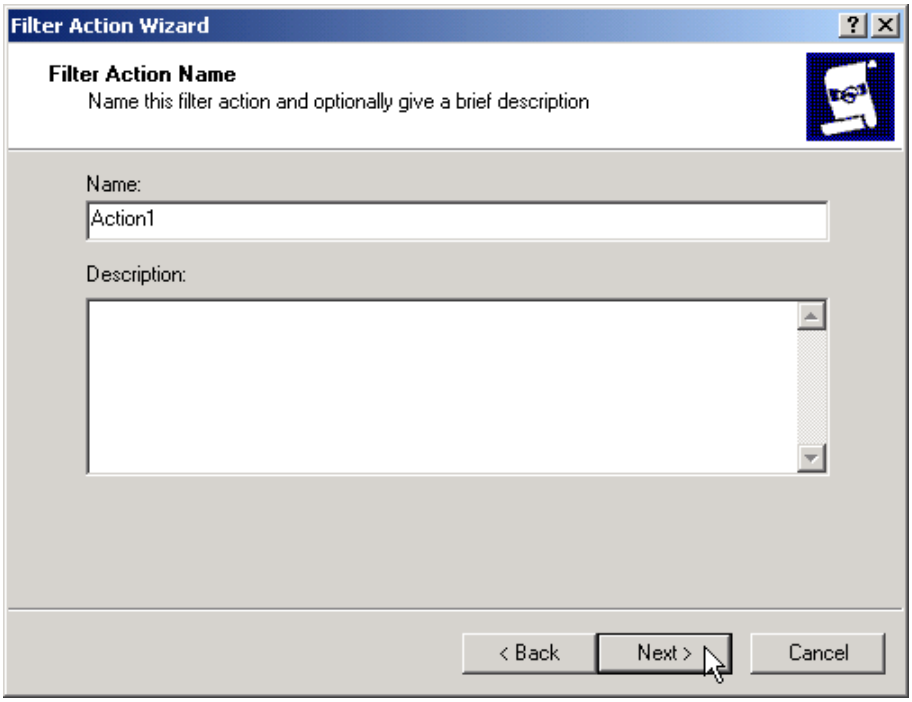


17. Click the **"Next"** button to continue.

Copyright 2003, ASUSTeK Computer, Inc.

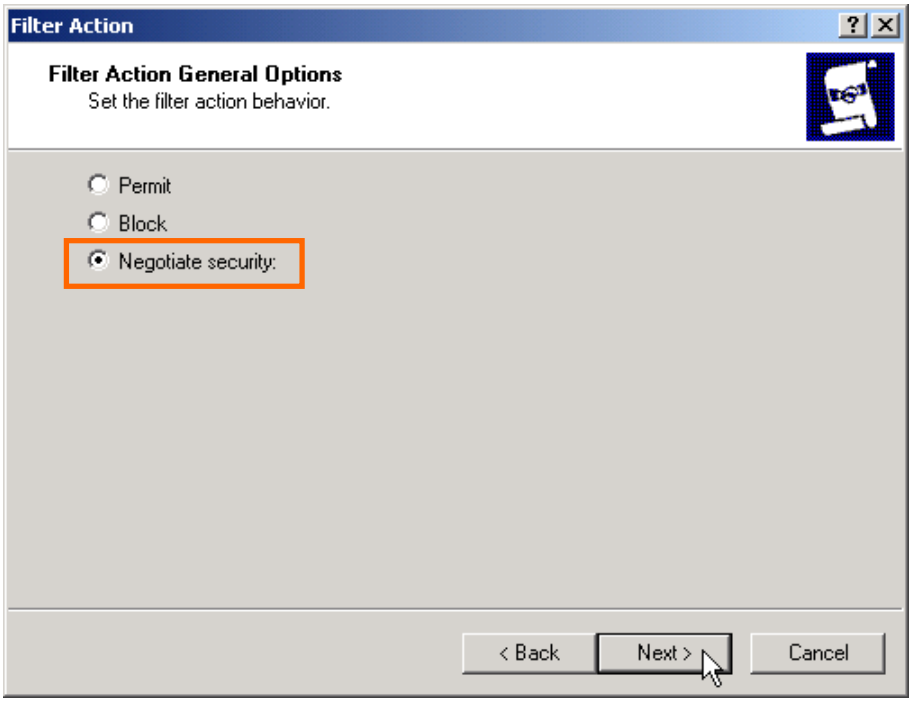


18. Name this filter action, **"Action1"**, and click the **"Next"** button to continue.

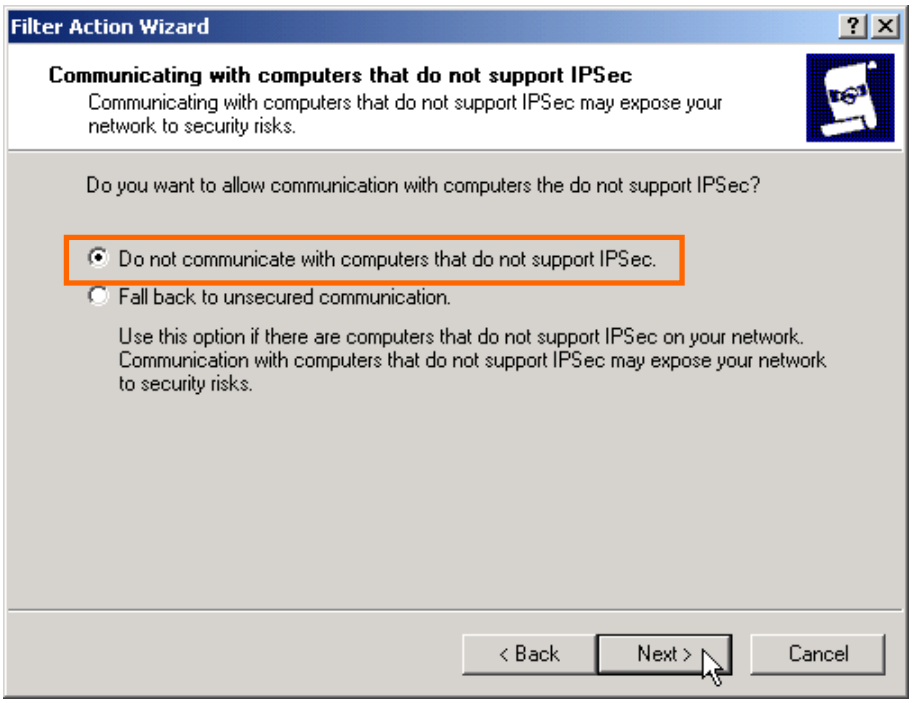


19. In the Filter Action General Options dialog box, select **"Negotiate security"**, and then click the **"Next"** button to continue.

Copyright 2003, ASUSTeK Computer, Inc.

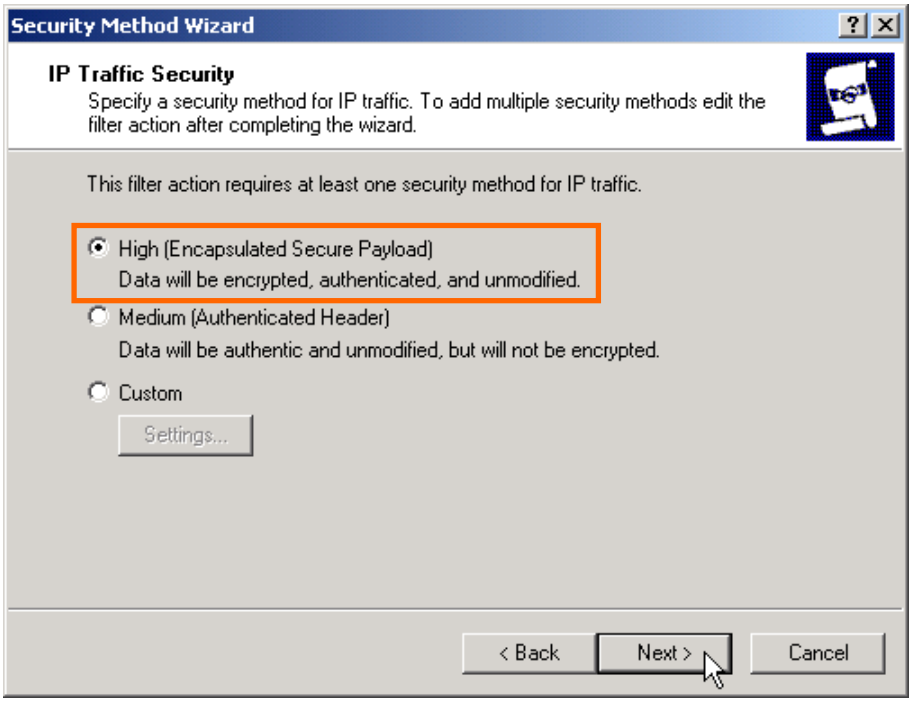


20. Select **"Do not communicate with computers that do not support IPSec"** from the "Filter Action Wizard" page, and then click the **"Next"** button to continue.

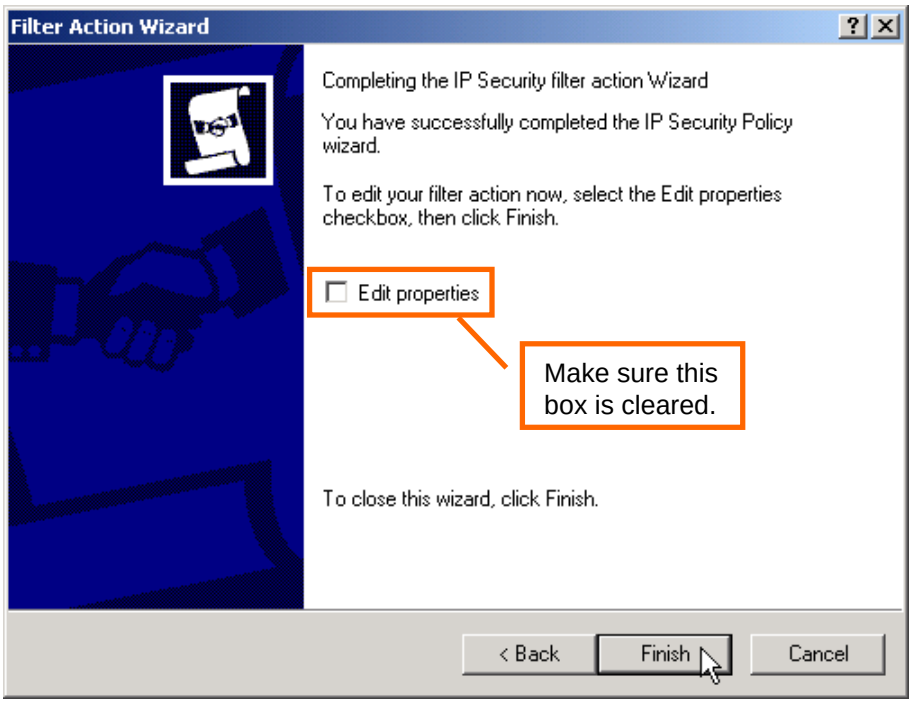


21. Select **"High {Encapsulated Secure Payload}"** from the list of security methods, and click the **"Next"** button to conitnue.

Copyright 2003, ASUSTeK Computer, Inc.

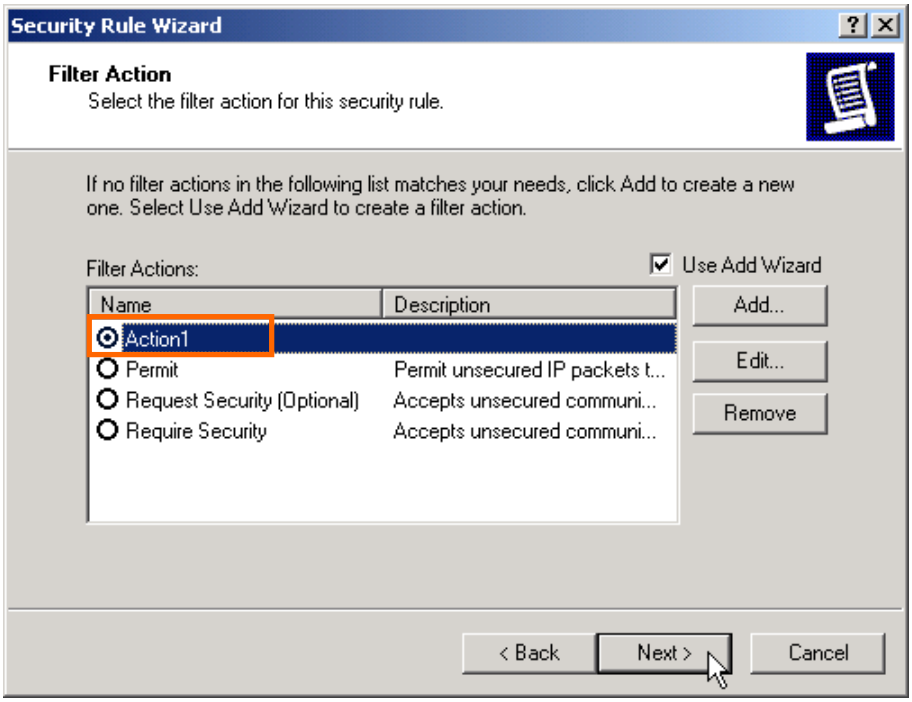


22. Make sure the **"Edit Properties"** check box is cleared (this is the default setting), and then click the **"Finish"** button to close "Filter Action Wizard" dialog box.

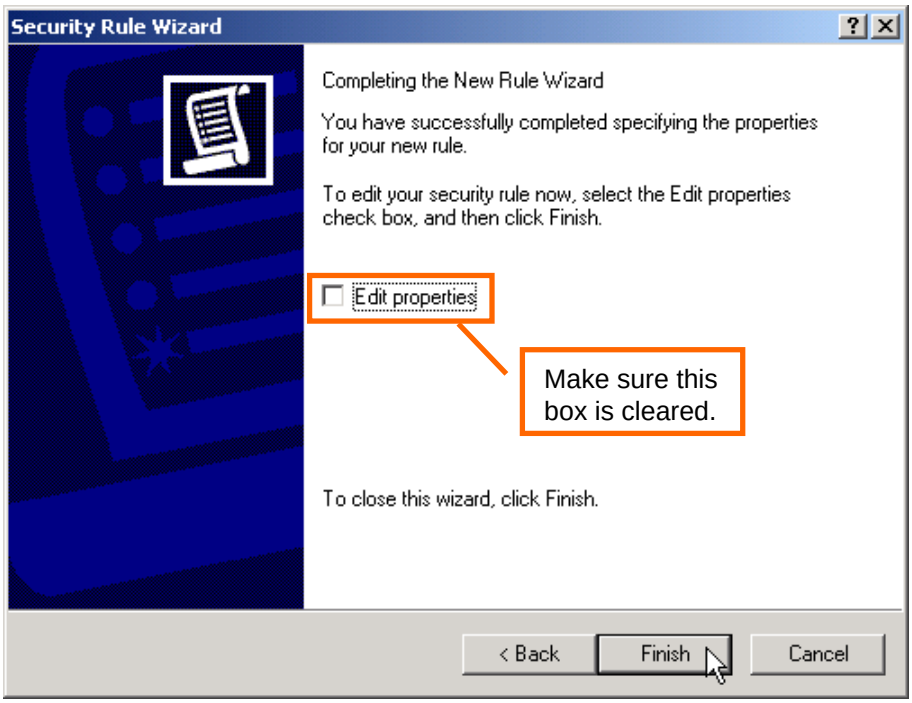


23. In the "Filter Action" dialog box, select "Action1" for this security rule and then click the **"Next"** button to close the Filter Action dialog box.

Copyright 2003, ASUSTeK Computer, Inc.



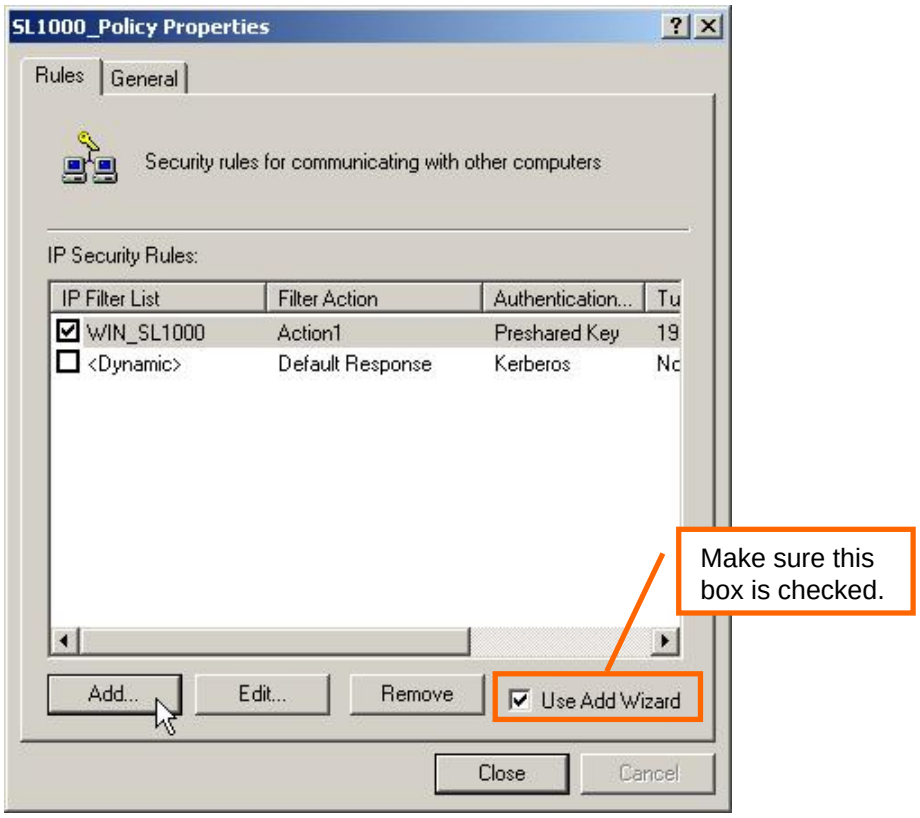
24. Make sure the **"Edit Properties"** check box is cleared (this is the default setting), and then click the **"Finish"** button to close the Security Rule Wizard.



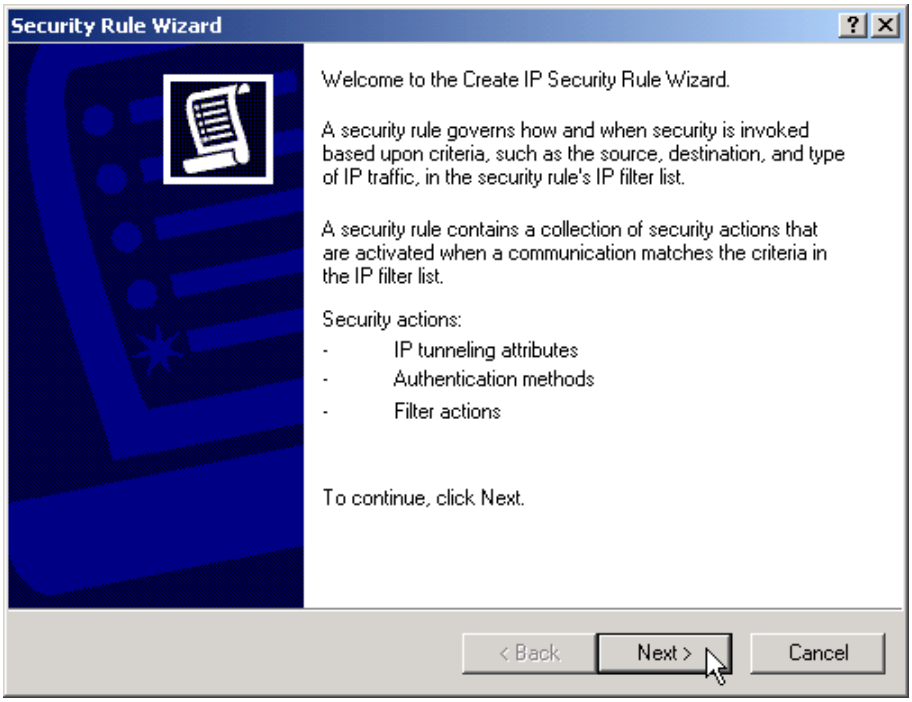
3.2.2 Configure an Inbound VPN Policy in Windows 2000/XP

1. Check the **"Use Add Wizard"** option and then click the **"Add"** button to create another IP Security Rule.

Copyright 2003, ASUSTeK Computer, Inc.

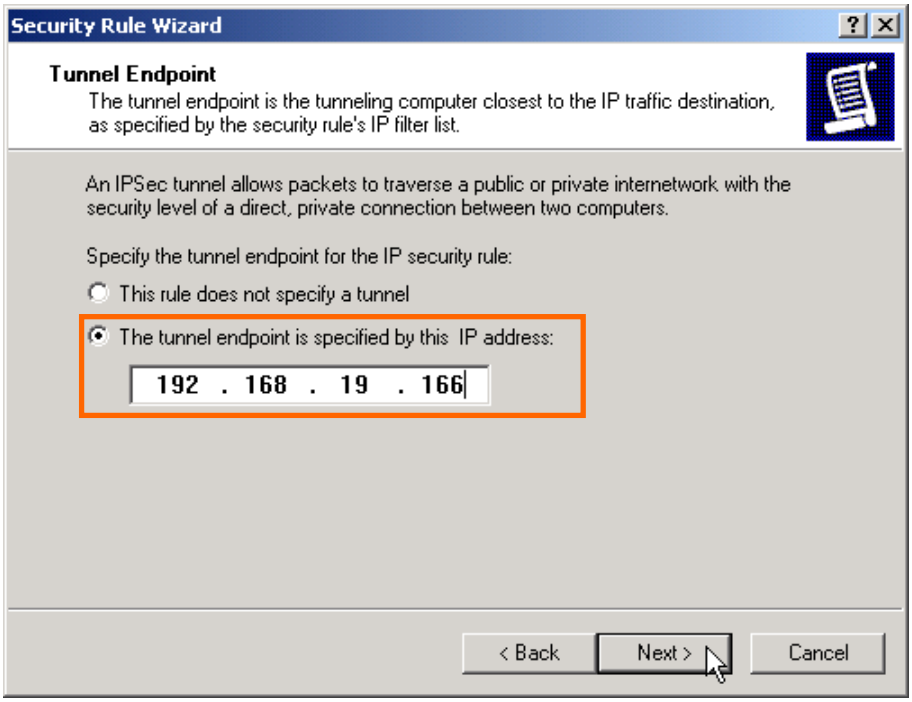


2. Click the **"Next"** button to continue.

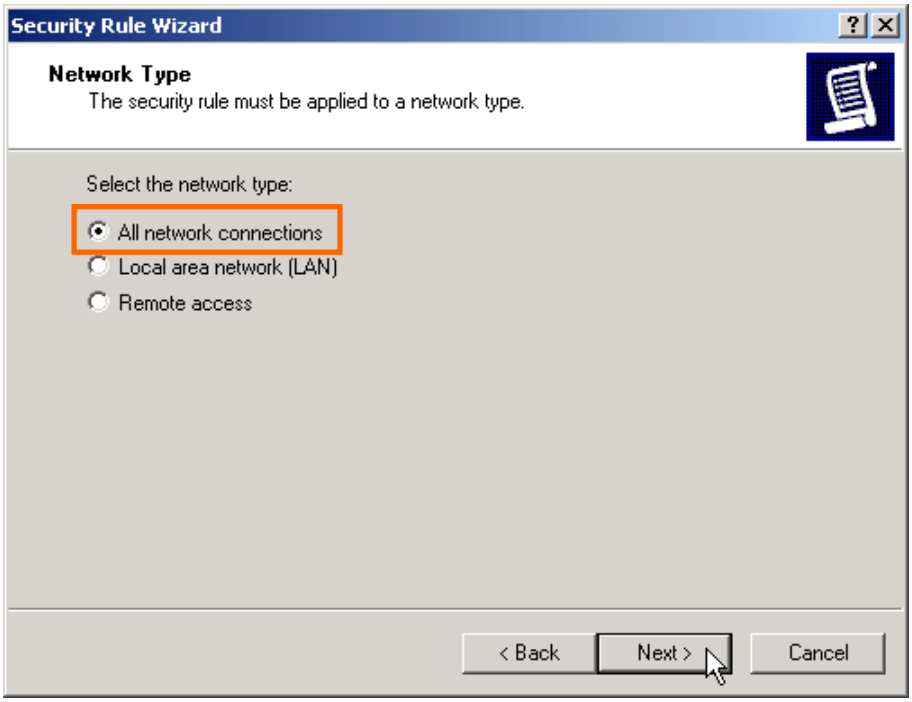


3. Select **"The tunnel endpoint is specified by this IP address:"**, enter **"192.168.19.166"** as the tunnel endpoint for this rule and then click the **"Next"** button to continue.

Copyright 2003, ASUSTeK Computer, Inc.

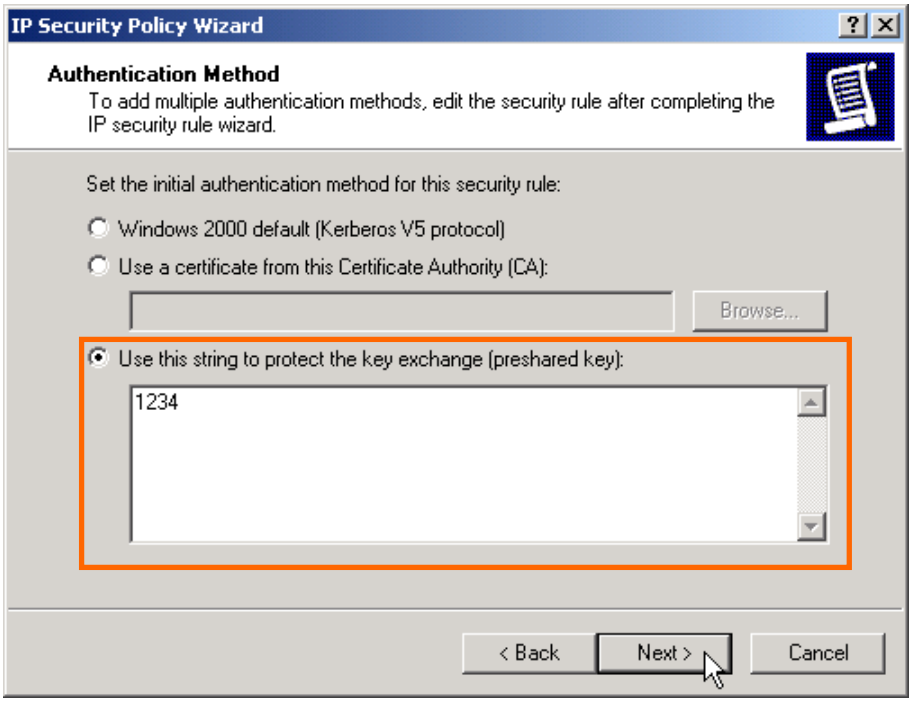


4. Select **"All network connections"** as the network type and then click the **"Next"** button to continue.

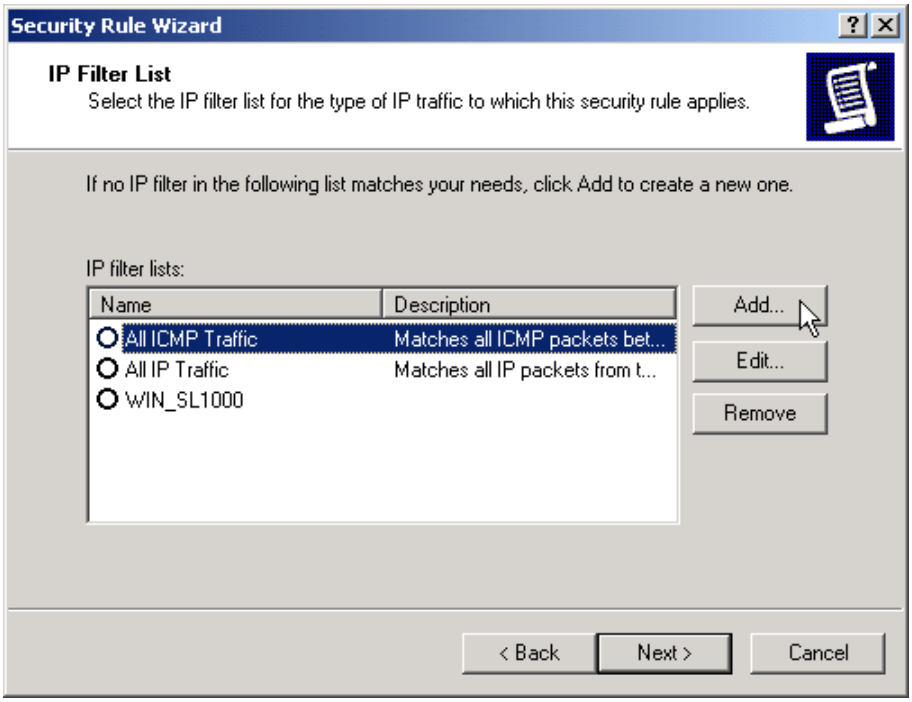


5. Select **"Use this string to protect the key exchange (preshared key):"** as the authentication method and enter **"1234"** as the preshared key. Make sure that this preshared key matches what is configured for the Internet Security Router. To make it more secure, you may choose a longer string. Note that you must not use a blank string for the preshared key. Click the **"Next"** button to continue.

Copyright 2003, ASUSTeK Computer, Inc.

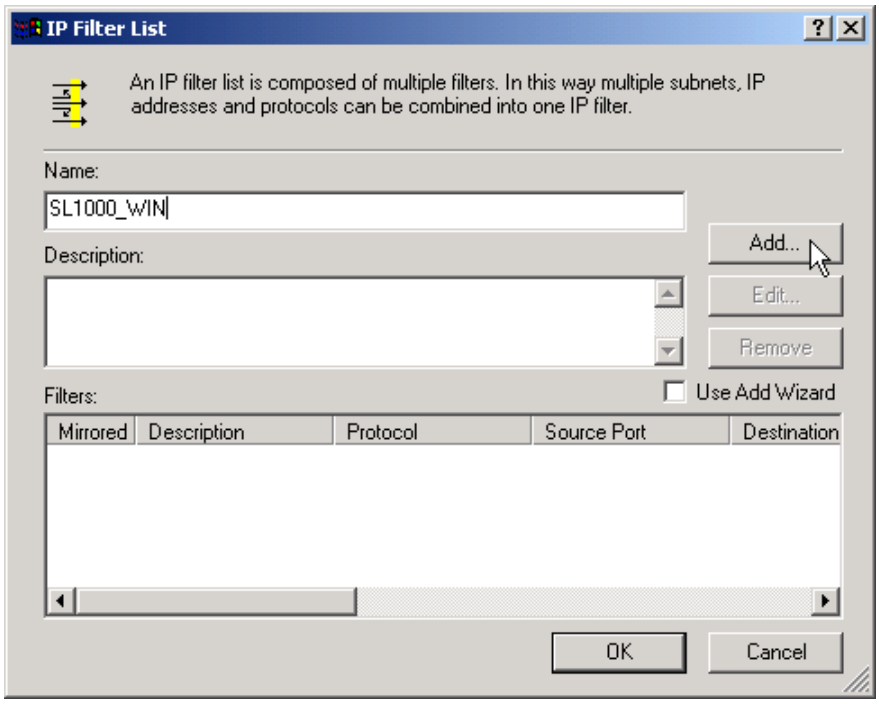


6. In the "IP Filter List dialog" box, click the **"Add"** button. A list of IP filter is displayed.

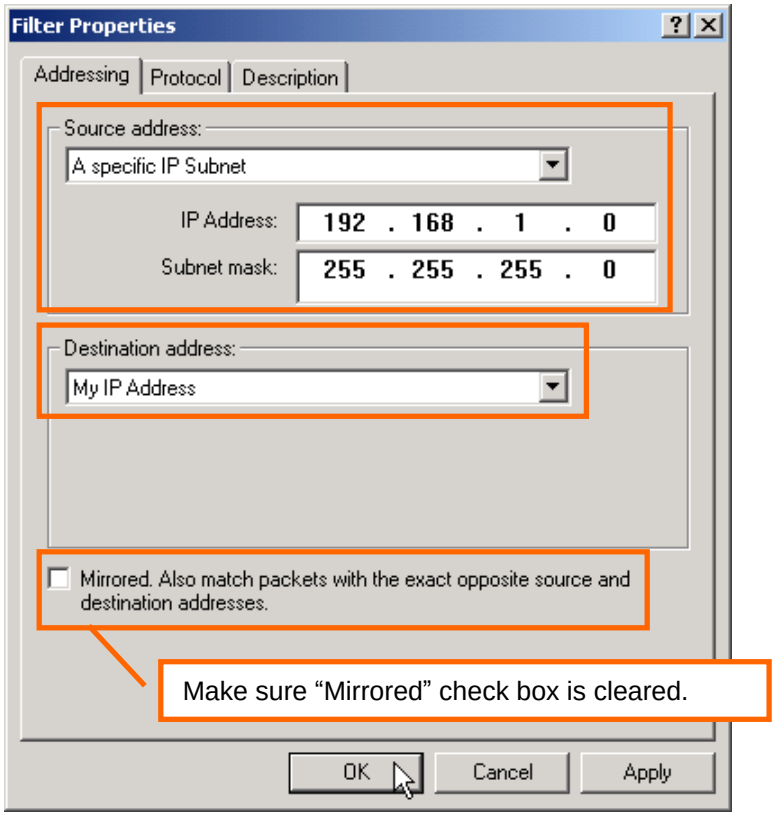


7. Name your filter, **"SL1000_WIN"**, and click the **"Add"** button to continue.

Copyright 2003, ASUSTeK Computer, Inc.

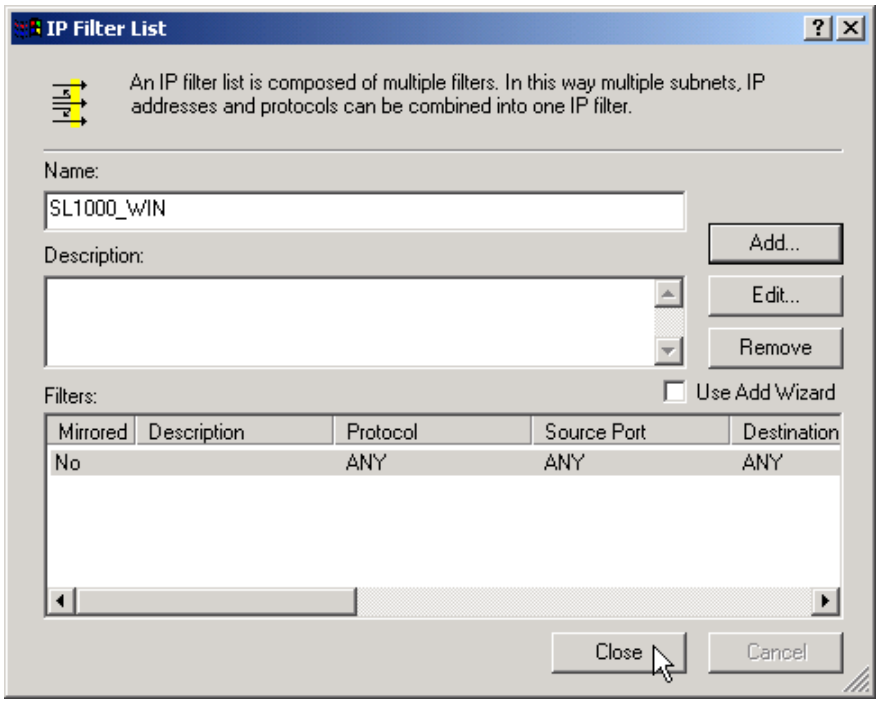


8. Select **"A specific IP Subnet"** from the "Source address:" drop-down list and enter **"192.168.1.0/255.255.255.0"** as the Source address and select **"My IP Address"** as the Destination address. Clear the **"Mirrored"** check box and then click the **"OK"** button to continue.

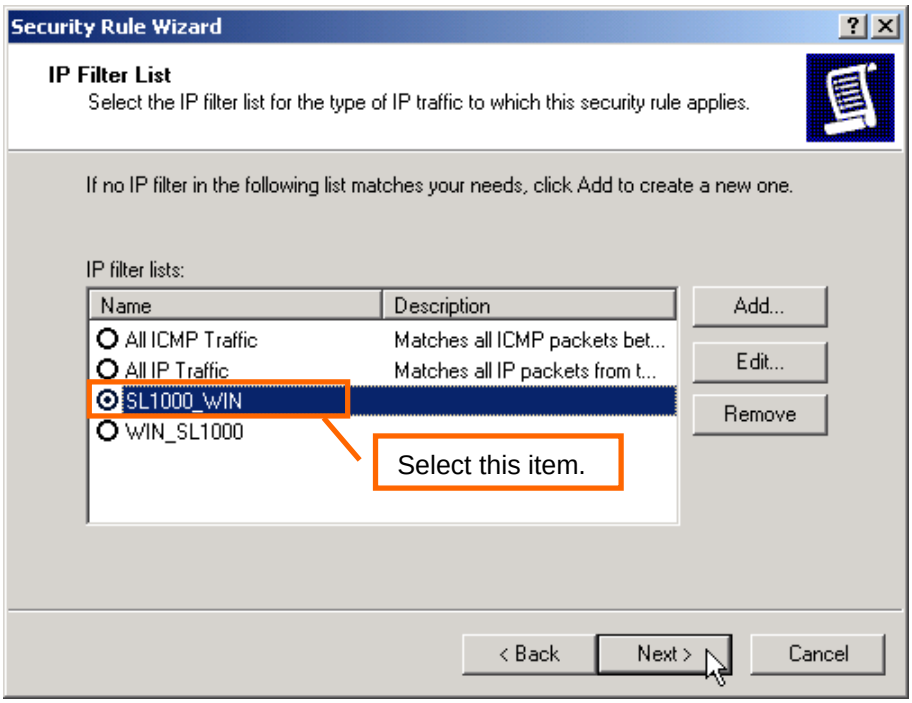


9. Click the **"Close"** button to close the "IP Filter List" dialog box.

Copyright 2003, ASUSTeK Computer, Inc.

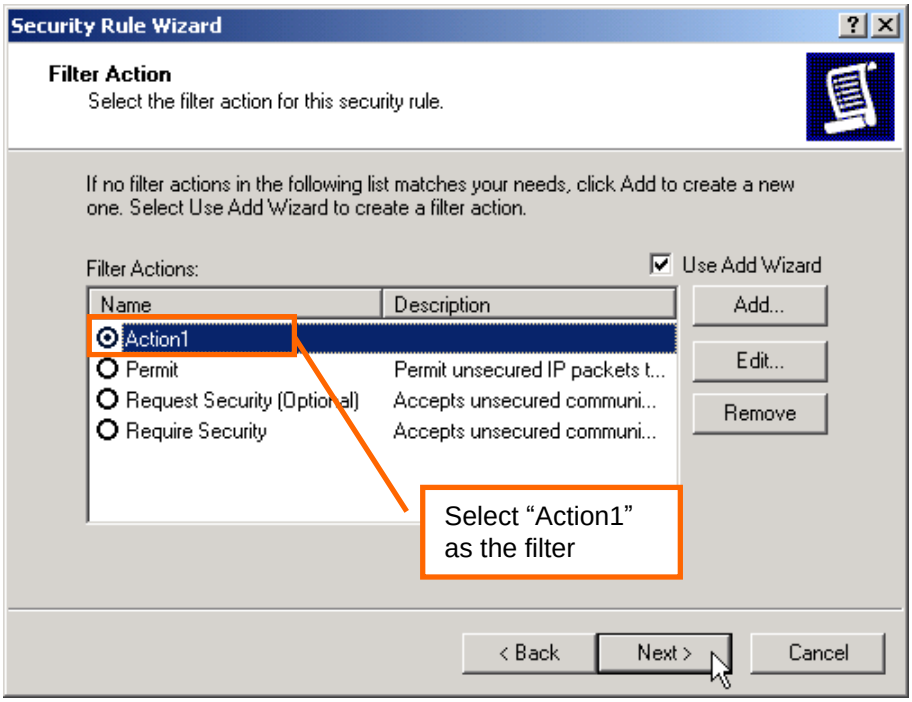


10. In the "Security Rule Wizard" dialog box, select the newly created security rule, **"SL1000_WIN"**, and click the **"Next"** button to configure Filter Action.

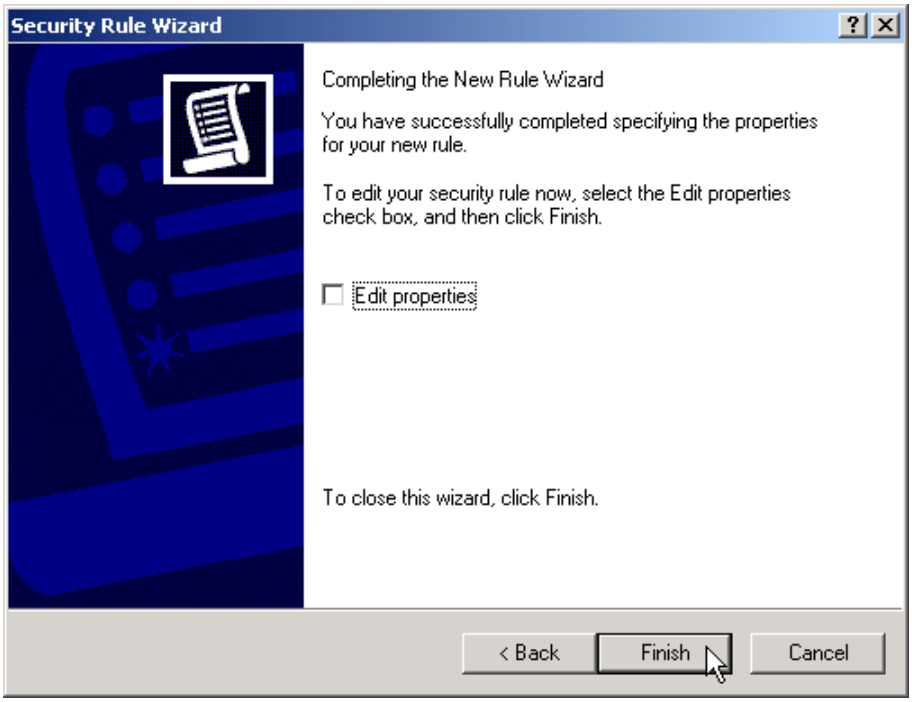


11. Select **"Action1"** as the filter action and then click the **"Next"** button to continue.

Copyright 2003, ASUSTeK Computer, Inc.

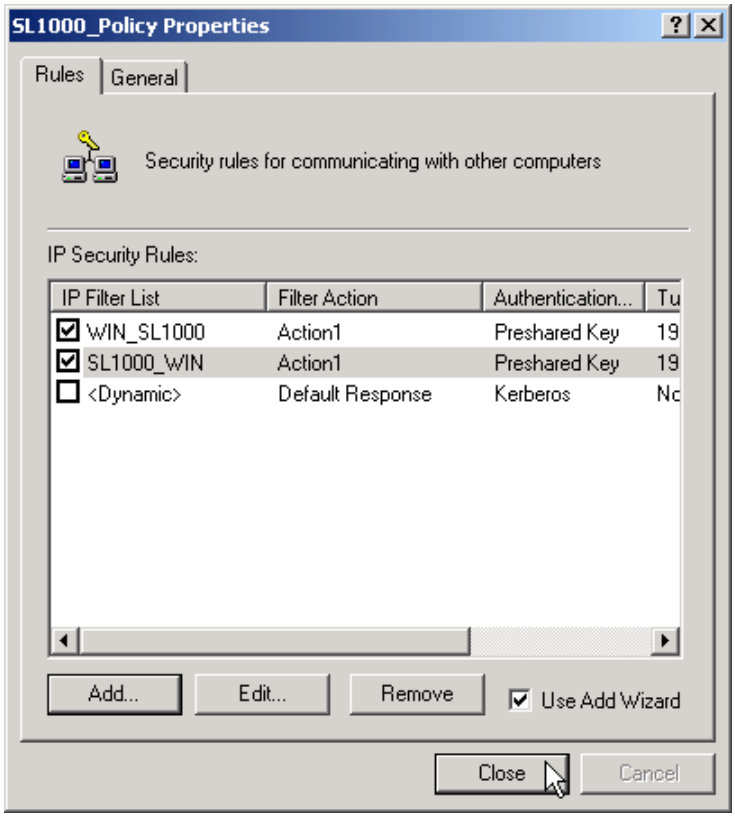


12. Click the **"Finish"** button to close the "Security Rule Wizard".

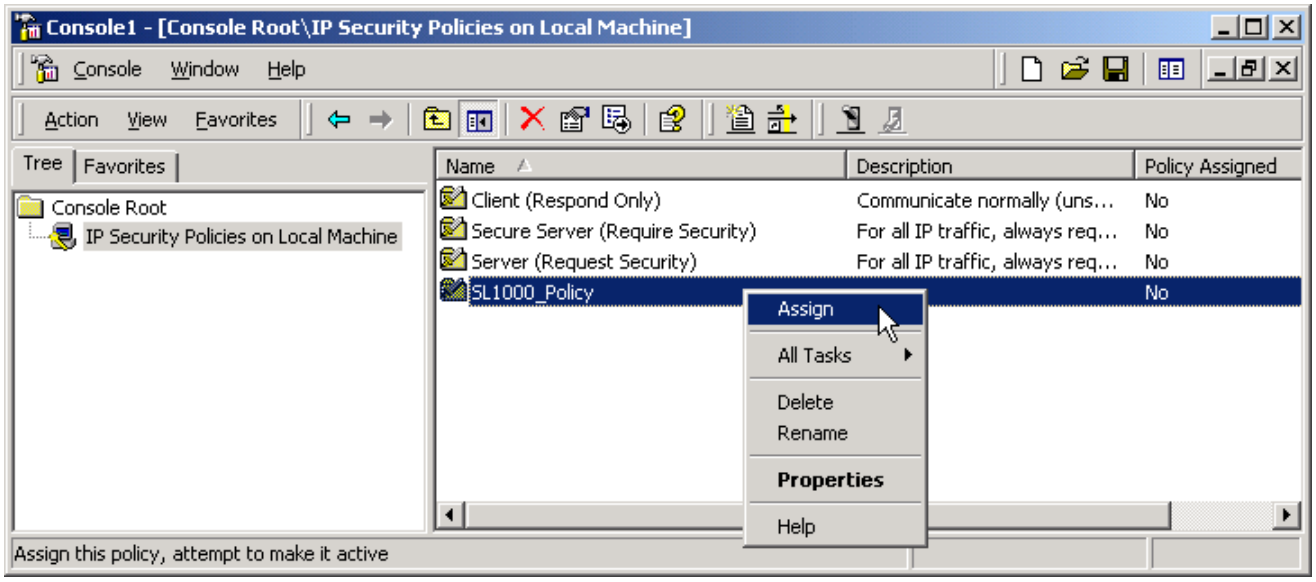


13. Click the **"Close"** button to complete the IPSec configuration task.

Copyright 2003, ASUSTeK Computer, Inc.

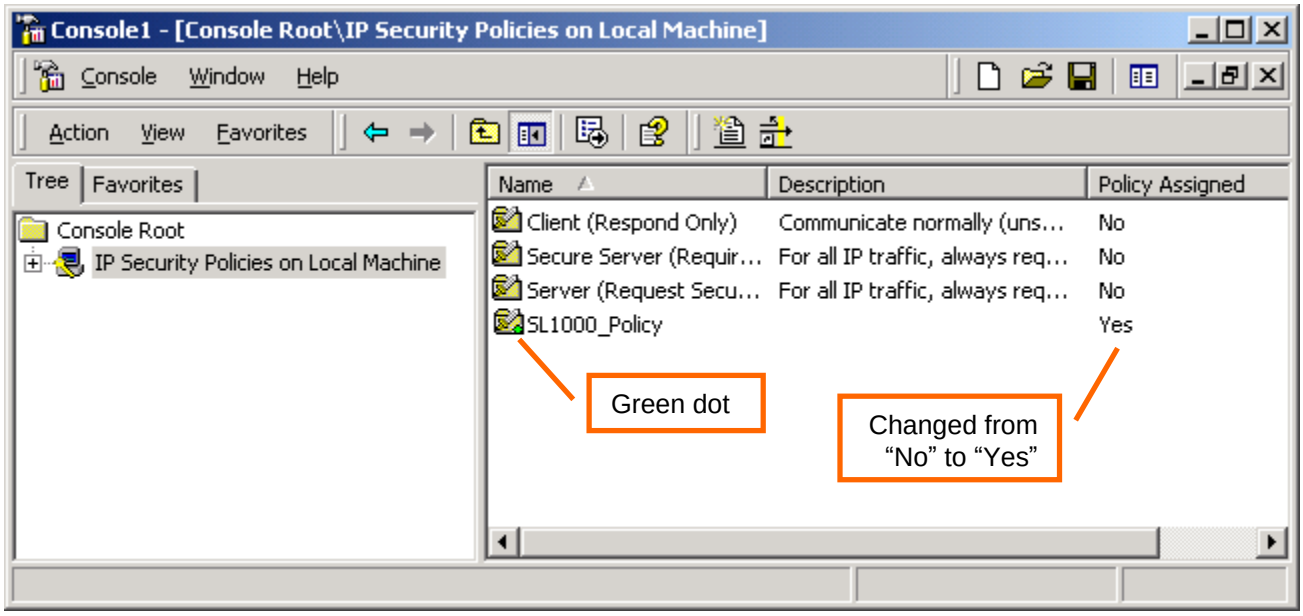


14. Right-click the **"SL1000_Policy"**, and select **"Assign"** from the context menu.



15. You can see that a green dot appears on the lower right corner of the icon. It identifies that "SL1000_Policy" has been assigned as an active IPSec policy. The status in the "Policy Assigned" column should change from "No" to **"Yes"**.

Copyright 2003, ASUSTeK Computer, Inc.



3.3 Configure the Internet Security Router

You need to login as admin to the Internet Security Router in order to configure the Internet Security Router. The procedure involves VPN policy setup, firewall outbound and inbound ACL rules.

3.3.1 Configure VPN Policy

Click the "VPN" menu and then click the "VPN Tunnel" submenu to access the VPN Tunnel configuration page. Configure the VPN policy based on the settings listed in Table 3.1. When done with the configuration, click the "Add" button to create the VPN policy. Please see Figure 3.1 for reference.

Table 3.1 VPN Policy Settings for the Internet Security Router

Field	Purpose	Value
Tunnel Name	Enter a unique name to identify the connection	SL1000_Policy
Site to Site radio button	Make it a site-to-site VPN connection	Selected
Local Secure Group	Select address, subnet or IP range	Subnet 192.168.1.0/255.255.255.0
Remote Secure Group	Select address, subnet or IP range	IP Address 192.168.19.166
Remote Gateway	Select Any, IP range or FQDN	IP Address 192.168.19.166
Preshared Key	A hexadecimal or ASCII shared secret	1234
IKE Mode	Select Main mode or Aggressive Mode	Main

Copyright 2003, ASUSTeK Computer, Inc.

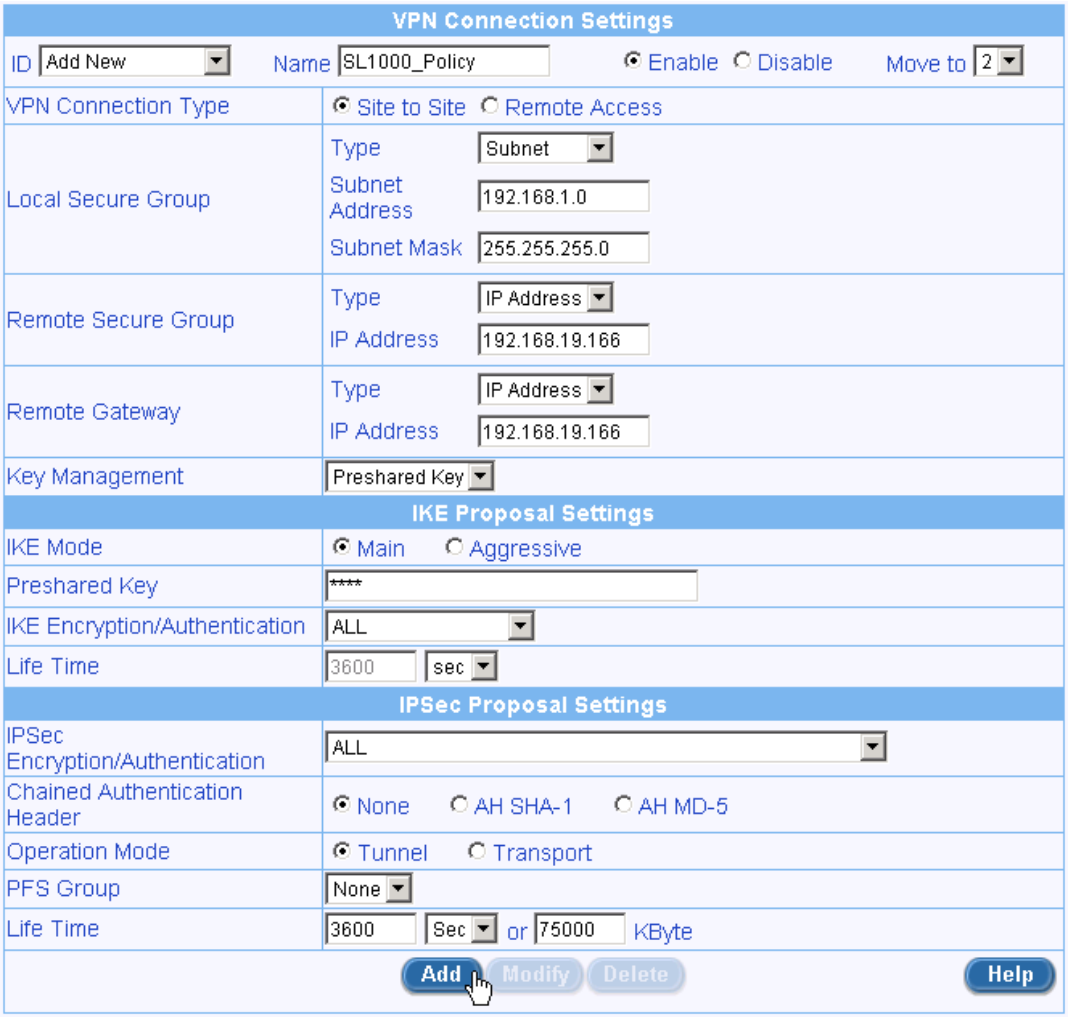


Figure 3.1. VPN Policy Configuration Settings

After the new VPN policy is created, you can see it displayed in the "Site to Site Access List Rules" as shown in Figure 3.2.

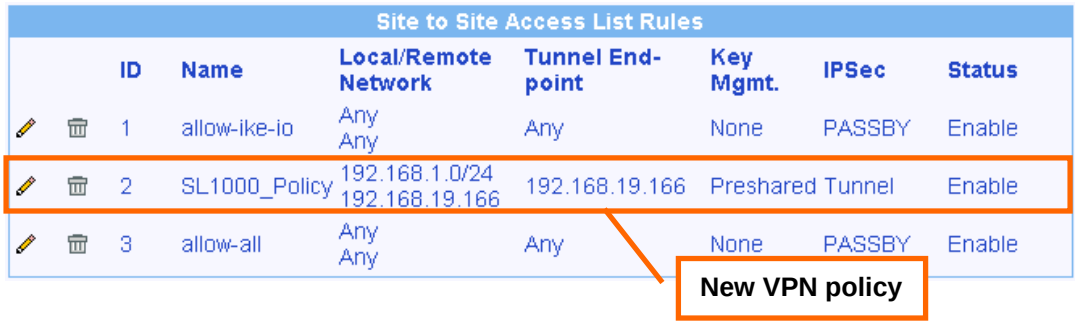


Figure 3.2. Verify the New VPN Policy

3.3.2 Configure an Outbound ACL Rule for the VPN Policy

This step is needed only when firewall is enabled. To allow outbound traffic to pass through the firewall, an outbound ACL rule is required; otherwise, the outbound traffic will be blocked by the firewall. Click the **"Firewall"**

Copyright 2003, ASUSTeK Computer, Inc.

menu and then click the **"Outbound ACL"** submenu to access the Outbound ACL configuration page. Enter the outbound ACL settings in the firewall Outbound ACL configuration page as shown in Figure 3.3. Click the **"Add"** button to create the new rule when done with the configuration. The newly created ACL rule will be displayed in the Outbound Access Control List table as shown in Figure 3.4.

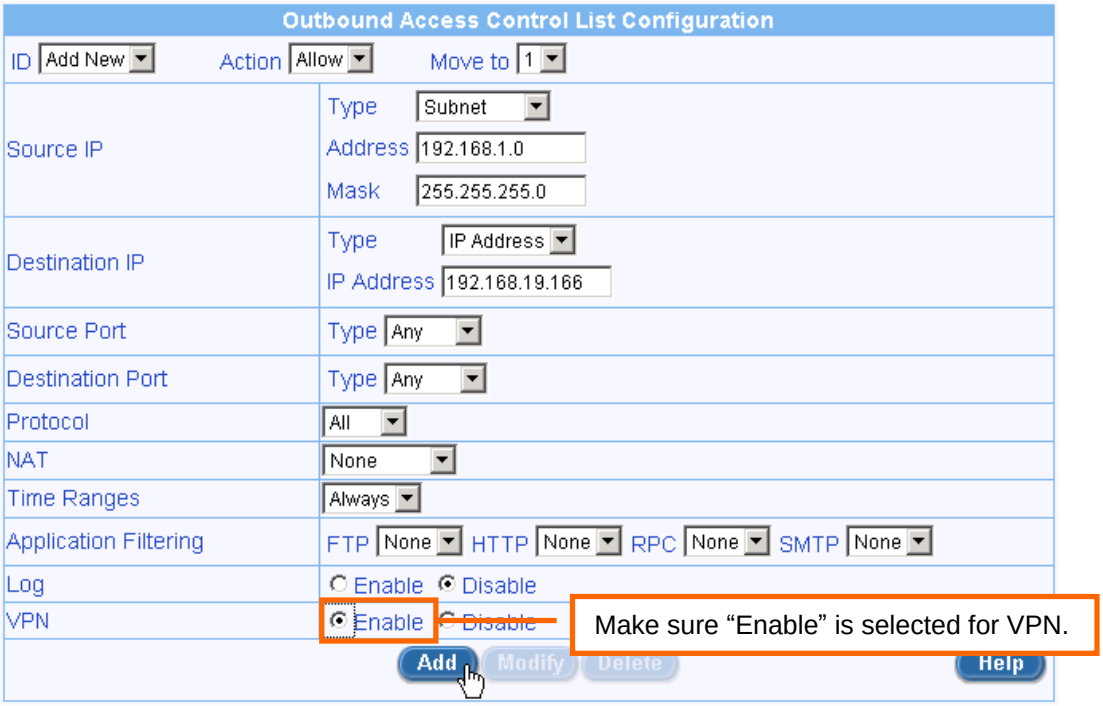


Figure 3.3. The Outbound ACL Rule Settings for the VPN Policy

Figure 3.4. Outbound ACL Summary

3.3.3 Configure an Inbound ACL Rule for the VPN Policy

This step is needed only when firewall is enabled. To accept the inbound traffic originated from the remote secure group, an inbound ACL rule is required; otherwise, the inbound traffic will be blocked by the firewall. Click the **"Firewall"** menu and then click the **"Inbound ACL"** submenu to access the Inbound ACL configuration page. Enter the inbound ACL settings in the firewall Inbound ACL configuration page as shown in Figure 3.5. Click the **"Add"** button to create the new rule when done with the configuration. The newly created ACL rule will be displayed in the Inbound Access Control List table as shown in Figure 3.6.

Copyright 2003, ASUSTeK Computer, Inc.

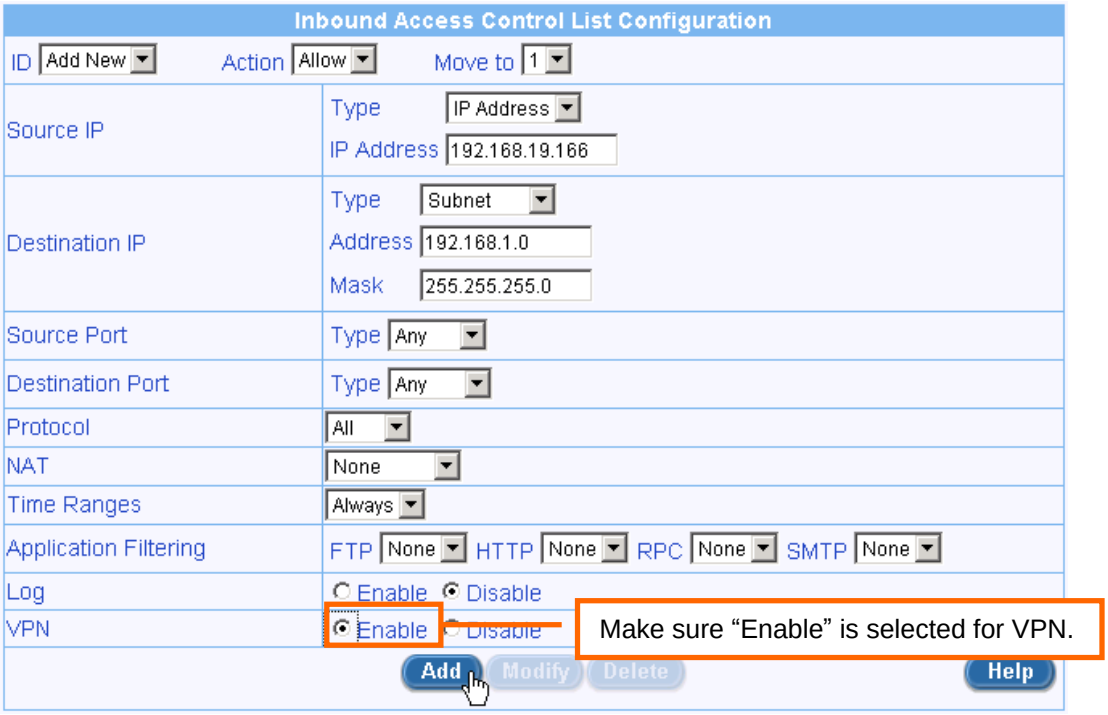


Figure 3.5. The Inbound ACL Rule Settings for the VPN Policy

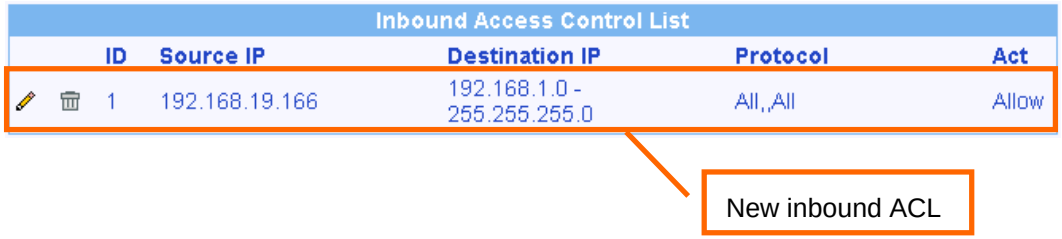


Figure 3.6. Inbound ACL Summary

4 Verify the IPSec VPN Connection

There are several ways to check if the IVPN connection is good or bad. You may start with the simplest tool (i.e. ping) to check if the VPN connection is OK and then venture into more complex tools to look for problems or find out details with the VPN connection.

4.1 ping

The “ping” program is the simplest utility to check if there is a connection between network nodes. However, ping alone cannot tell what is wrong with the connection if there is a problem with the connection. You can open a “Command Prompt” window, as shown in the following figure, and ping PC1 from PC2 by entering “ping 192.168.1.10” (assuming IP of PC1 is 192.168.1.10) or ping PC2 from PC1 by entering “ping 192.168.19.166” at the command prompt to check if the VPN connection is established. You will receive several “Negotiating IP Security” responses initially (if you ping PC1 from PC2) during the negotiation of IPSec VPN tunnel. Repeat the “ping” command, and you will receive successful ping responses in a few more tries.

Copyright 2003, ASUSTeK Computer, Inc.

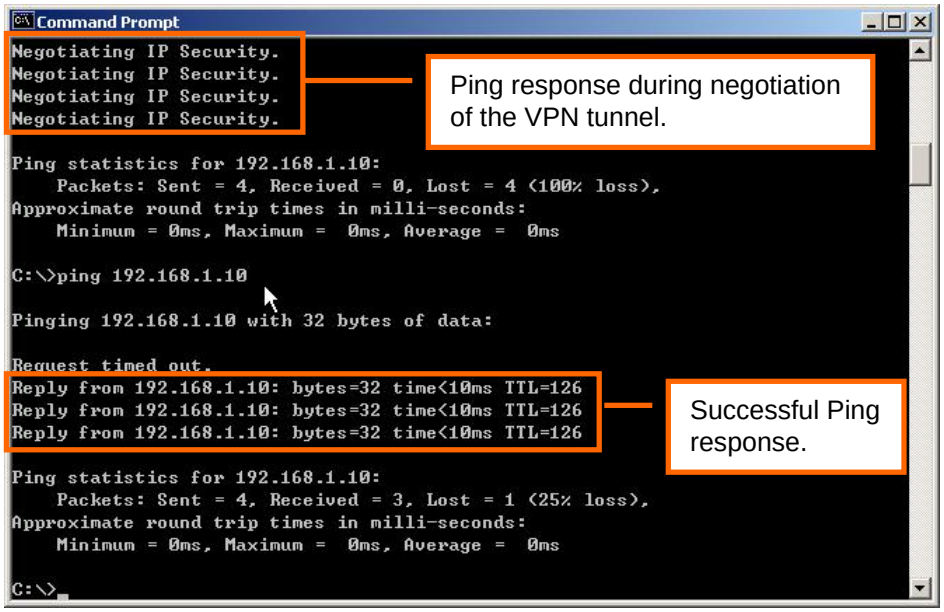


Figure 4.1. Ping Example for Verifying IPSec VPN Connection

4.2 Monitor IPSec VPN Traffic on the Internet Security Router

The Internet Security Router comes with the monitoring tool for the IPSec VPN traffic. Click the VPN menu and then click the “Statistics” submenu to see the VPN Statistics page, as shown in Figure 4.2. This page shows information regarding IKE (Internet Key Exchange) and IPSec. You may use it to find out problems w/ the IPSec traffic. For example, if there is a problem during IKE, the “Phase1 Status” column will display a message for the problem. To find out details on IPSec SA (security association), click the icon to display the IPSec SA page as shown in Figure 4.3.

Copyright 2003, ASUSTeK Computer, Inc.

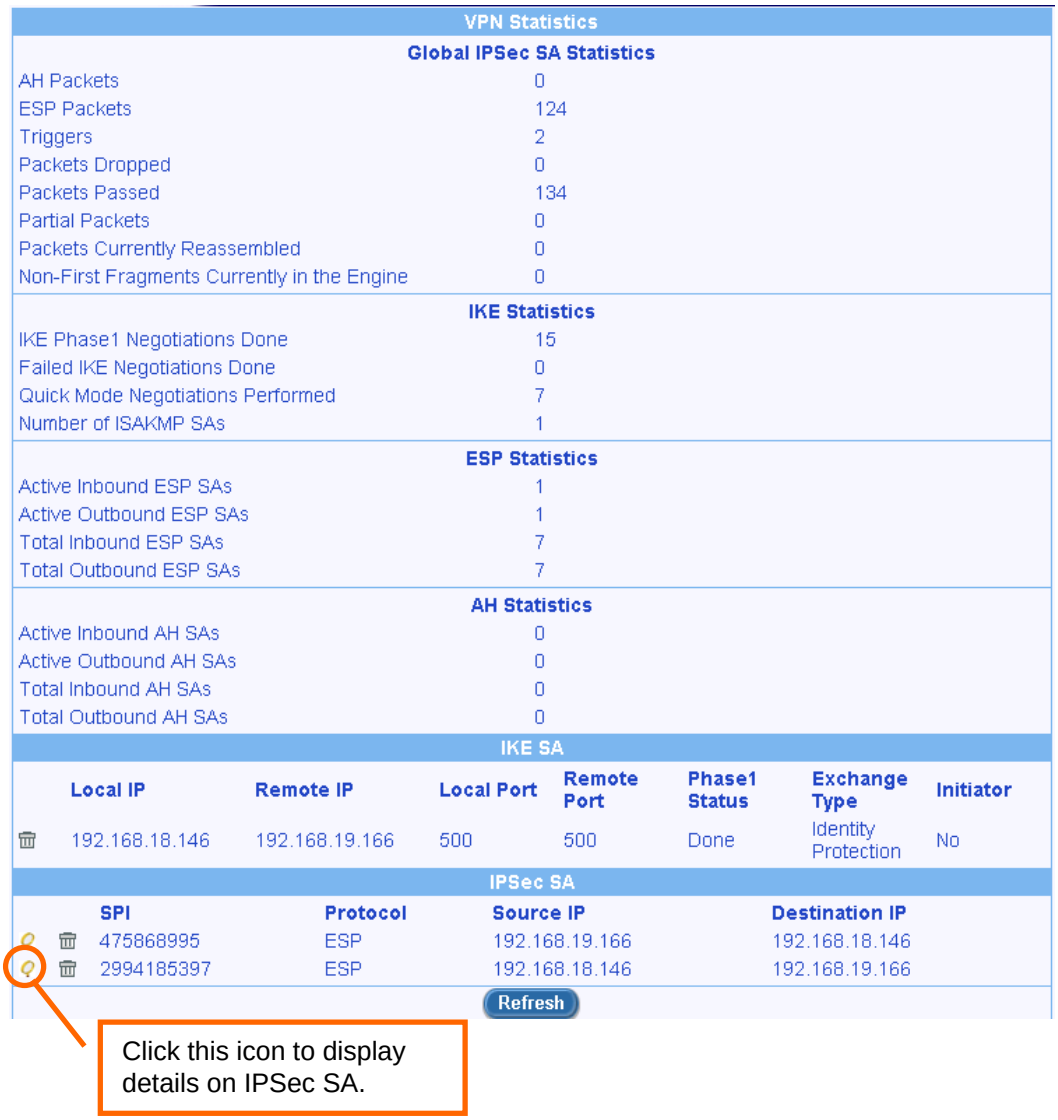


Figure 4.2. VPN Statistics on the Internet Security Router

Copyright 2003, ASUSTeK Computer, Inc.

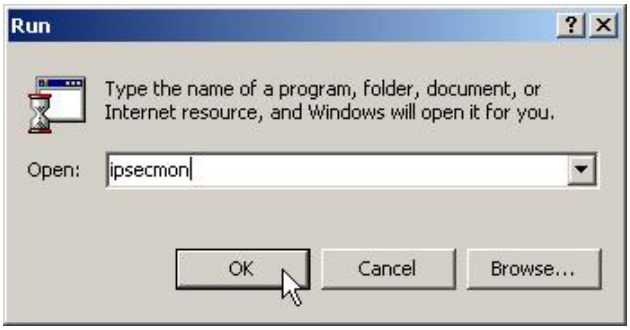
IPSec SA	
SPI	2994185397
Protocol	ESP
Direction	Outgoing
Local Secure Group	Type Subnet Subnet IP 192.168.1.0 Subnet Mask 255.255.255.0
Remote Secure Group	Type IP Address IP Address 192.168.19.166
Source Port	ANY
Destination Port	ANY
Source Protocol	ANY
Destination Protocol	ANY
Source Tunnel Address	192.168.18.146
Destination Tunnel Address	192.168.19.166
Bundle	7
Operation Mode	Tunnel
Authentication algorithm	SHA
Encryption algorithm	3DES
Creator of the SA	IKE
Life Times	3600 Secs. 75000 Kilo Bytes
OK	

Figure 4.3. IPSec SA Example

4.3 ipsecmon

4.3.1 Windows 2000

Windows 2000 includes a program called ipsecmon for monitoring the IPSec VPN traffic. If you cannot find it in your computer, you may download it from Microsoft website. This program provides details about your IPSec VPN traffic, such as IPSec/IKE statistics, information about connecting parties and etc. To run ipsecmon, click "Start", click "Run", enter "ipsecmon" in the "Run" dialog box and then click the "OK" button.



The IP Security Monitor is then displayed as shown in Figure 4.4.

Copyright 2003, ASUSTeK Computer, Inc.

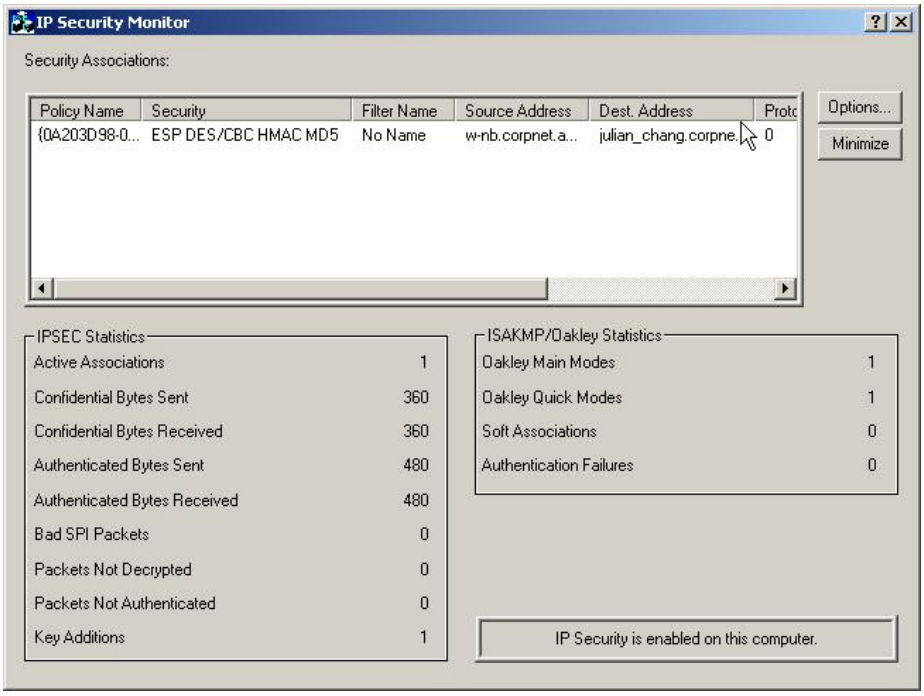
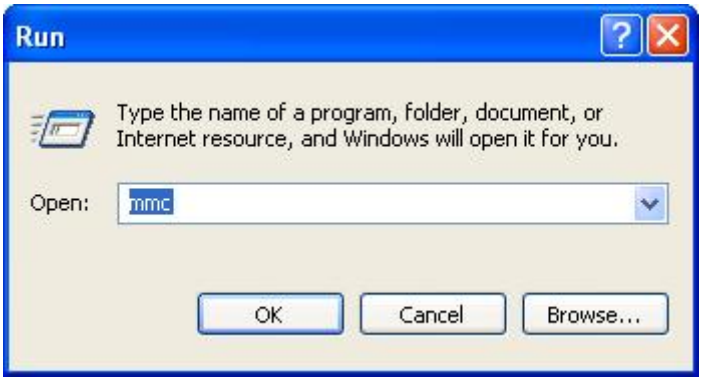


Figure 4.4. IP Security Monitor Example

4.3.2 Windows XP

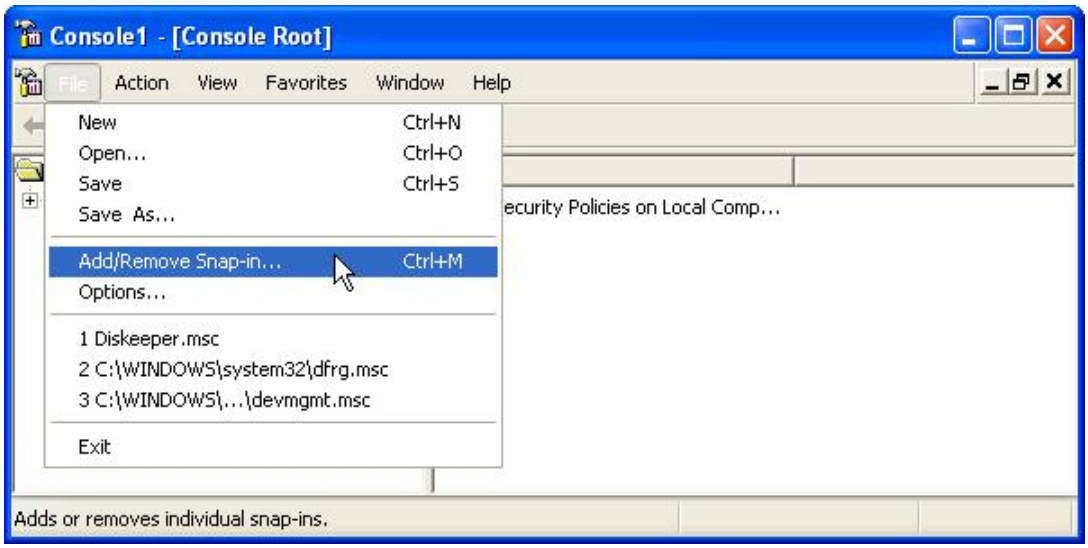
For Windows XP, ipsecmon is integrated into MMC console. Follow the instructions below to install and use ipsecmon.

1. Start the MMC console: From the Windows desktop, click on **"Start"**, and then click on **"Run"**. Enter **"mmc"** in the pop-up "Run" dialog window (as shown in the figure below) and then click on the **"OK"** button to continue.

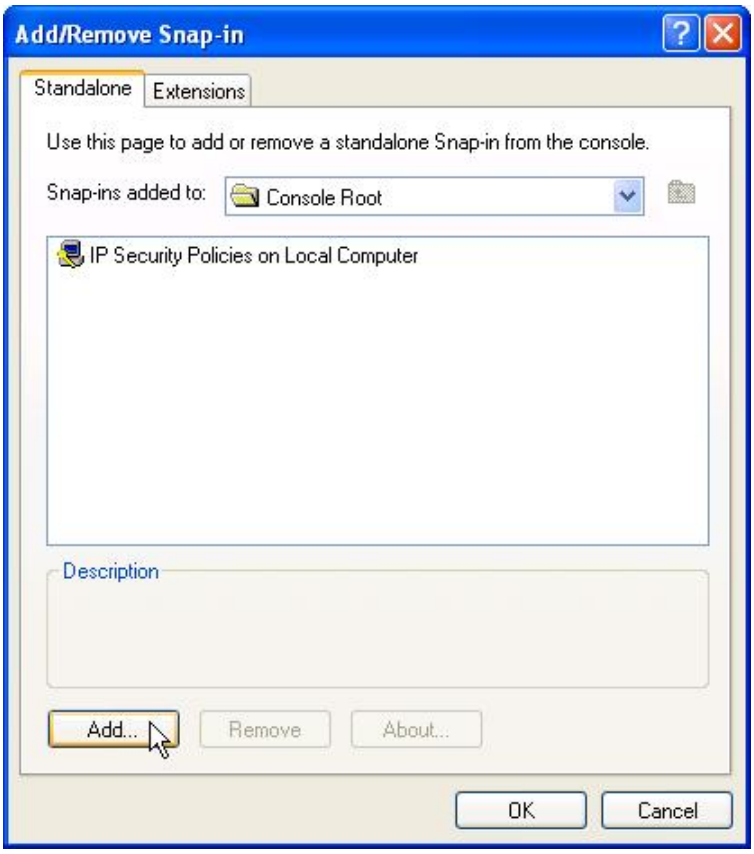


2. The MMC console window displays. Click on the **"Console"** menu, and then select the **"Add/Remove Snap-in…"** submenu.

Copyright 2003, ASUSTeK Computer, Inc.

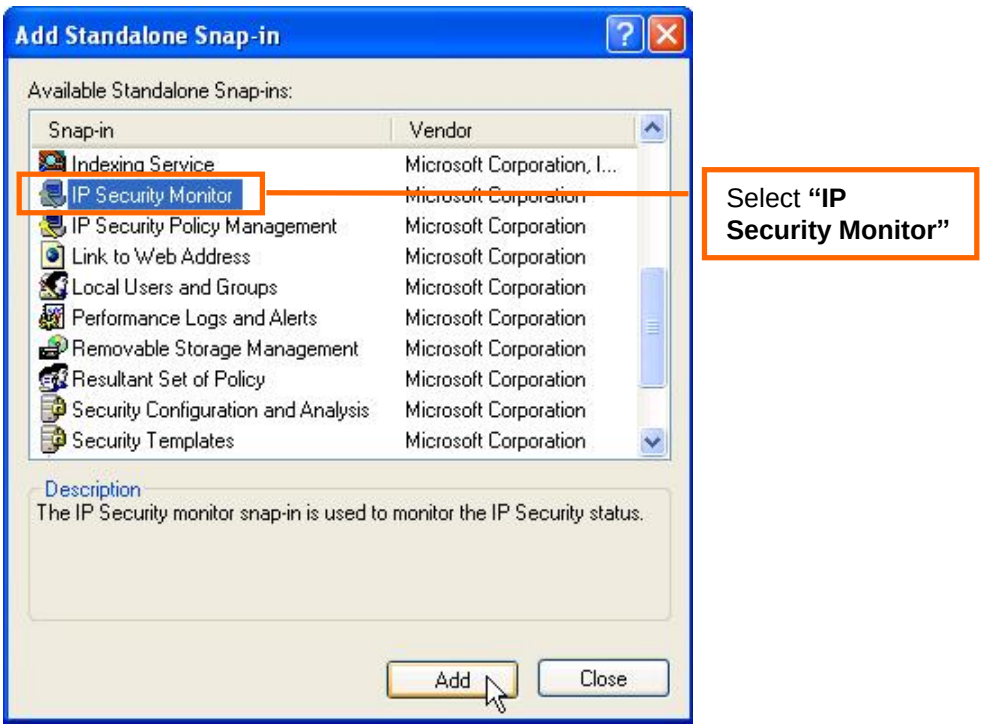


3. In the Add/Remove Snap-in dialog box, click on the **"Add"** button to continue.



4. In the Add Standalone Snap-in dialog box, select **"IP Security Monitor"** (you may need to scroll down the list to see this item) and then click on the **"Add"** button to continue.

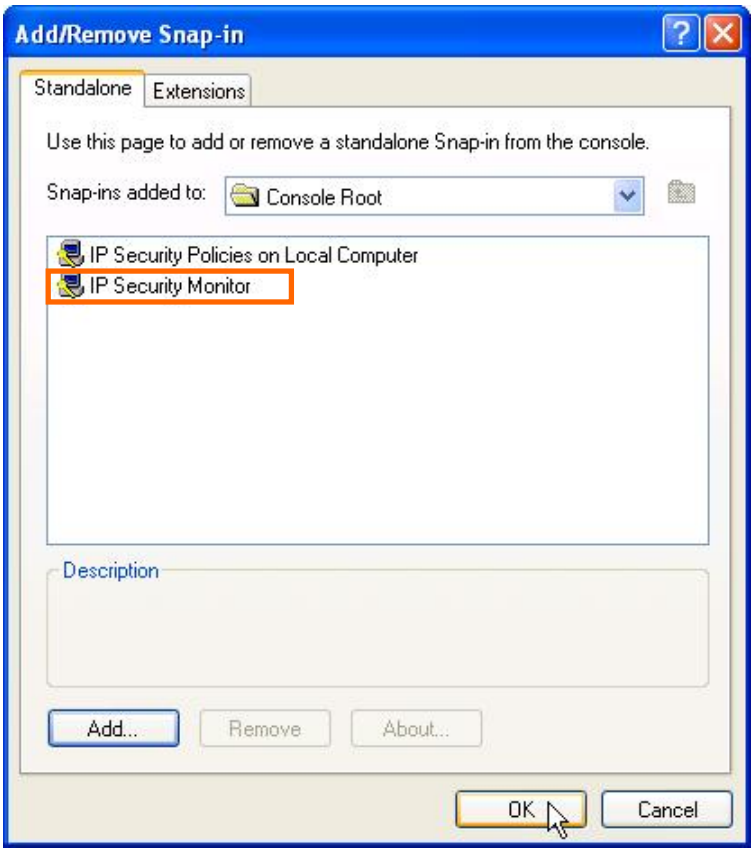
Copyright 2003, ASUSTeK Computer, Inc.



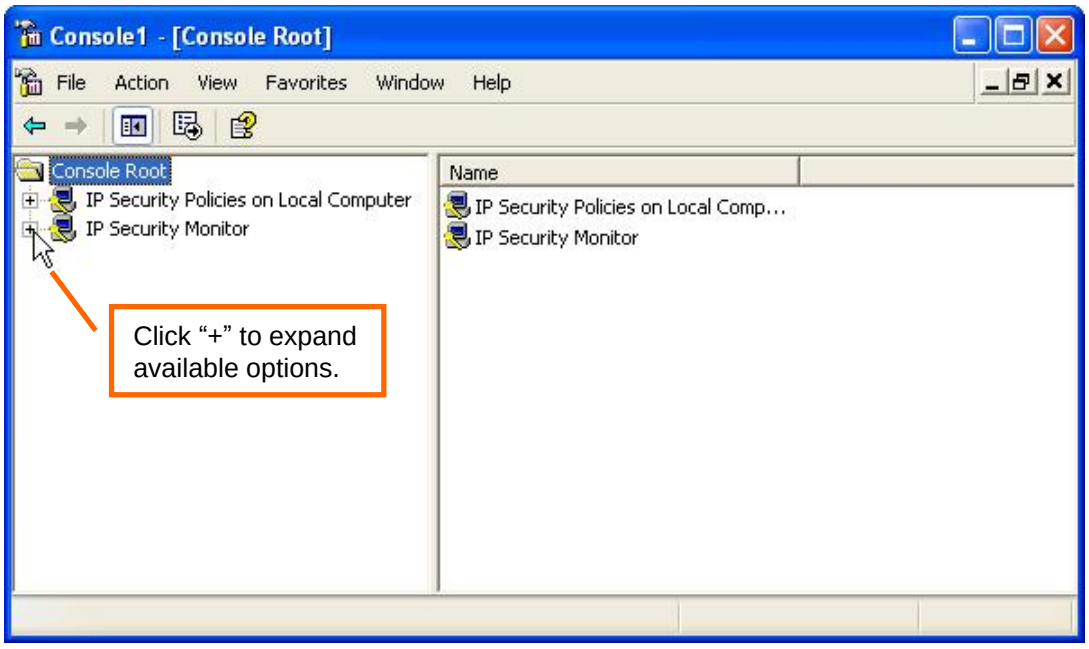
5. Click the **"Close"** button.

6. You can see that "IP Security Monitor" is added. Click the **"OK"** button to return to the MMC console window.

Copyright 2003, ASUSTeK Computer, Inc.

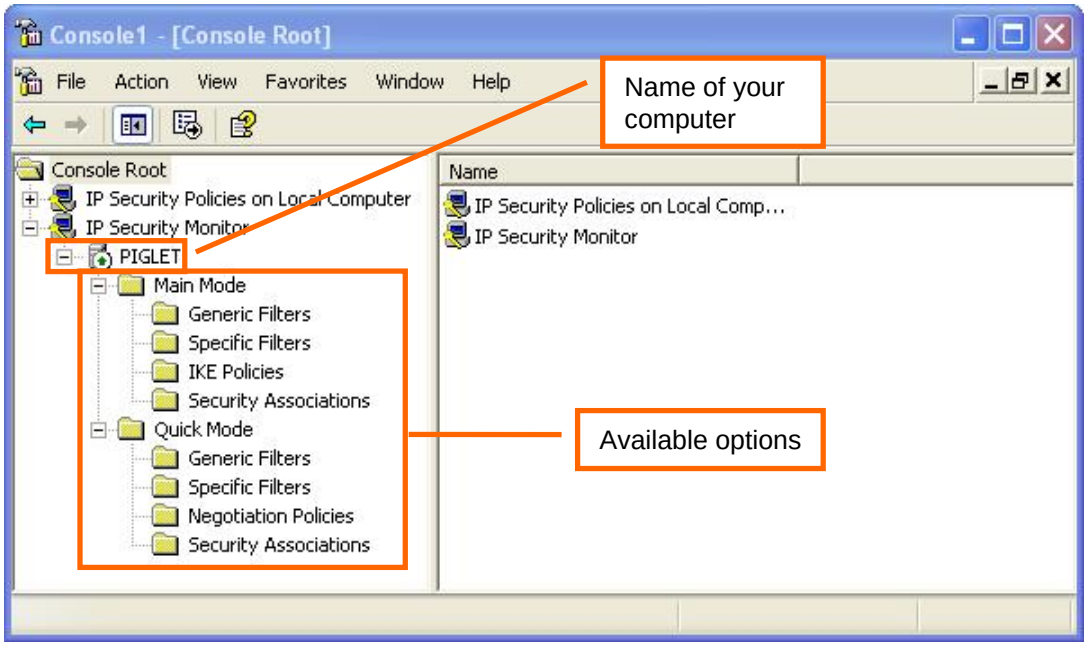


7. MMC console displays. Click on the "+" symbol to expand available options for "IP Security Monitor".



8. The following figure shows all the available options for IP Security Monitor. You may click any of the options to find out detail information regarding your IPSec VPN connection.

Copyright 2003, ASUSTeK Computer, Inc.



Copyright 2003, ASUSTeK Computer, Inc.